Security Gateway Configuration Guide

Models: SG-5110, SG-3110, SG-5105

CONFIGURATION GUIDE

Contents

Chapter 1 Application Acceleration Configuration....1
1 Configuring VWAN....2
2 Configuring HT TP-AD....15
3 Configuring APP-CACHE....22
Chapter 2 Application Configuration....33
1 Configuring Network Communication Test Tools....34
2 Traceroute Test....35
3 Configuring DHCP....46
4 Configuring DNS....77
5 Configuring DDNS....83
6 Configuring NTP....88
7 Configuring SNTP....102
8 Configuring DNS Proxy....108
9 Configuring FTP Server....120
10 Configuring Time Range....129
11 Configuring SMART-DNS....133
Chapter 3 Basic Management....138
1 Configuring CLI....139
2 Configuring Basic Management....151
3 Configuring Lines....178
4 Configuring Password Policy....185
5 Configuring Software Authorization Management....191
6 Configuring PKG_MGMT....203
7 Configuring CWMP....220
8 Configuring Syslog....240
9 Configuring LED....291
10 Configuring Exception Alarm....295
11 Configuring HTTP Service....305
12 Configuring PATCH-UPGRADE....319
13 Configuring WEB-UPGRADE....324
Chapter 4 Behavior Management....328
1 Configuring Layer 2/3 Classification....329
2 Configuring APP-IDENTIFY....356
3 Configuring APP-ROUTE....381
4 Configuring APP-PROXY....398
5 Configuring User Session Limit....403
6 Configuring Flow Control....419
7 Configuring Flow Audit....438
8 Configuring Content Audit....451
9 Configuring LINE-QUALITY....551
Chapter 5 Device Management....560
1 Configuring Device Audit....561

2 Configuring USB....566
3 Configuring User Task....573
4 Configuring SERVICE-MANAGER....581
Chapter 6 IP Address & Application Configuration....585
1 Configuring IP Addresses and Services....586
2 Configuring ARP....609
3 Configuring IP Event Dampening....632
4 Configuring TCP....637
5 Configuring IPv4/IPv6 REF....649
6 Configuring Tunnel Interfaces....655
7 Configuring FPM....673
8 Configuring NAT....685
9 Configuring MLLB....717
10 Configuring USER-ROUTE....735
Chapter 7 IPv6 Configuration....749
1 Configuring IPv6....750
Chapter 8 Network Management Configuration....794
1 Configuring RLOG....795
2 Configuring POLICE-LOG....810
3 Configuring LOG-POLICY....837
4 Configuring SNMP....843
5 Configuring CM-APM....871
6 Configuring ANTI-SNIPER....889
Chapter 9 Reliability Configuration....902
1 Configuring VRRP....903
2 Configuring RNS....935
Chapter 10 Routing Configuration....958
1 Configuring PBR....959
2 Configuring ROUTE-DB....974
3 Configuring RIP....981
4 Configuring RIPng....1026
5 Configuring OSPFv2....1046
6 Configuring OSPFv3....1123
7 Managing Routes....1194
Chapter 11 Security Configuration....1214
1 Configuring the ACL....1215
2 Configuring RPL....1236
3 Configuring RNFP....1240
4 Configuring SSH....1260
5 Configuring DHCP Snooping....1295
6 Configuring ARP Check....1312
7 Configuring IP Source Guard....1320
8 Configuring SEC-VPDN....1327
9 Configuring IPSec....1364

10 Configuring IKE.....1386
11 Configuring ITBOX.....1403
12 Configuring AAA.....1408
13 Configuring RADIUS.....1453
14 Configuring TACACS+.....1478
15 Configuring Web Authentication.....1489
16 Configuring Global IP-MAC Binding.....1561
17 Configuring IPoE.....1569
18 Configuring IP Group.....1575
19 Configuring Link SAM.....1580
20 Configuring FLOW ACCOUNT.....1588
21 Configuring APP-AUTH.....1595
22 Configuring Webservice.....1653
23 Configuring ANTI-PAP.....1658
24 Configuring WEB-ADVERT.....1664
25 Configuring Local-Account.....1671
26 Configuring the Firewall.....1679
Chapter 12 WLAN QoS Configuration.....1727
1 Configuring WQoS.....1728
2 Configuring WMM.....1739
Chapter 13 WLAN RF Configuration.....1755
1 Configuring WLAN Optimization.....1756
2 Configuring Band Select.....1814
Chapter 14 WLAN Security Configuration.....1824
1 Configuring RSNA.....1825
2 Configuring WIDS.....1843
Chapter 15 WLAN Basic Configuration.....1875
1 Configuring APMG.....1876
2 Configuring STA Management.....1918
3 Configuring CAPWAP.....1946
4 Configuring WBS.....1985
5 Configuring ETH-MNG.....2034
6 Configuring DATA-PLANE.....2041
7 Configuring WLOG.....2047
Chapter 16 Interface Configuration.....2054
1 Configuring Interfaces.....2055
2 Configuring MODE-MGMT.....2079
3 Configuring DLDP.....2101
4 Configuring PCAP.....2108
5 Configuring PPPOE-CLIENT.....2114
6 Configuring PPPoE Server.....2125
7 Configuring Aggregated Port.....2140
8 Configuring VLAN-TERMINAL.....2151

Chapter 1 Application Acceleration Configuration

1. Configuring VWAN
2. Configuring HTTP-AD
3. Configuring APP-CACHE

1 Configuring VWAN

1.1 Overview

WAN Virtualization (VWAN), also referred to as pipe acceleration, is an acceleration technology deployed at both ends. It is used to optimize data transmission between devices in the headquarters and branches of an enterprise.

VWAN establishes VWAN channels and virtual links between devices in the headquarters and branches of an enterprise, to form accelerated pipes. Key service data flows of an enterprise that match the Access Control List (ACL) or server addresses are transmitted to VWAN channels. Encapsulated using the Multilink Protocol (MP), key service data flows are transmitted via different virtual links to achieve the multilink bundling function. The multilink bundling function differs from the multilink load balancing function. The multilink bundling function enables a single data flow to overcome the bandwidth restriction of a single physical link, and transmits data flows at a rate approximate to the total bandwidth of multiple links. In addition, the VWAN adopts the adaptive Forward Error Correction (FEC) technology and packet re-order technology, to eliminate packet loss and disorder in the WAN, thereby improving the transmission rate and transmission quality for data flows of key services.

VWAN mainly implements multilink bundling.

Multilink bundling: Used in scenarios in which the enterprise headquarters use high-bandwidth and high-quality links (such as fiber links) whereas branches use multiple low-bandwidth links (such as ADSL dialup links) to access the WAN.

1.2 Applications

Application	Description
Applying Multilink Bundling	Bundles and aggregates the bandwidth of multiple physical links to overcome bandwidth restriction of a single link.

1.2.1 Applying Multilink Bundling

Scenario

Multilink bundling needs to be enabled on links between devices in the headquarters and branches of an enterprise.

As shown in Figure 1-1:

The enterprise headquarters use two high-bandwidth and high-cost links to access the WAN, for example, fiber links that provide 10 Mbps uplink bandwidth and 10 Mbps downlink bandwidth. The ISPs of the two links are ISP-1 and ISP-2.

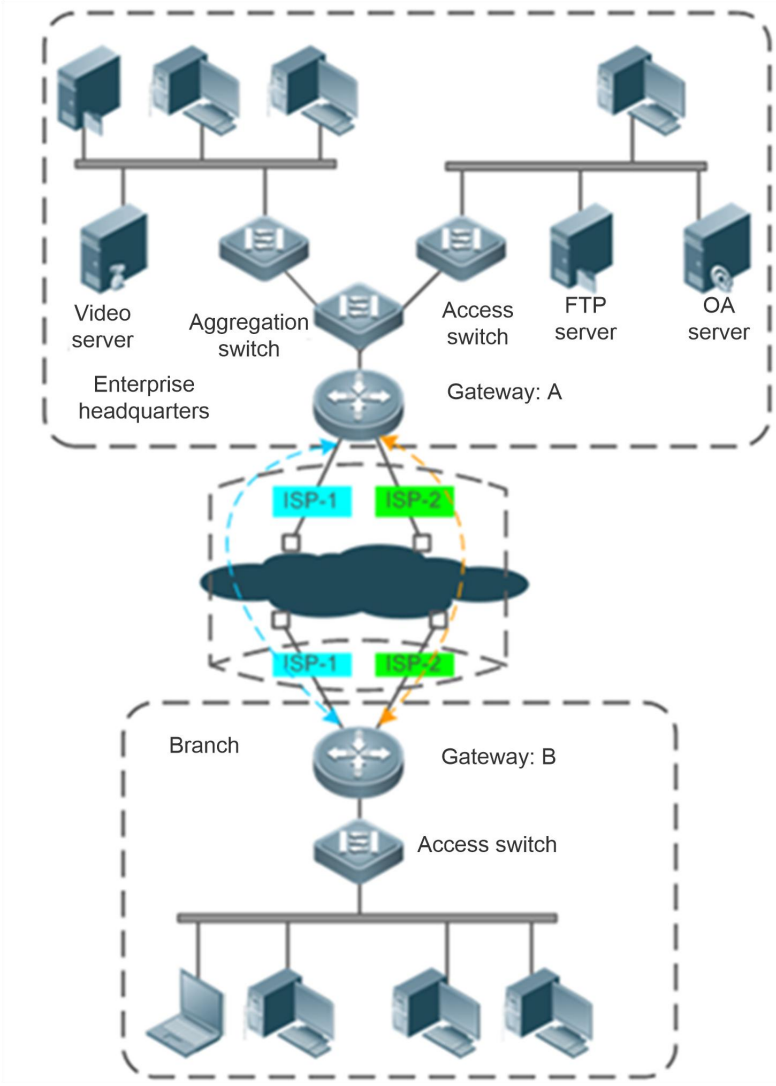
The branch uses two low-bandwidth and low-cost links to access the WAN, for example, ADSL dialup links that provide 2 Mbps uplink bandwidth and 512 kbps downlink bandwidth. The ISPs of the two links are ISP-1 and ISP-2.

Key service servers such as the OA system server and video conference server are deployed in the headquarters.

In an example of a video conference, a high-definition video conference needs links to provide 1 Mbps uplink and downlink bandwidth. However, the uplink bandwidth of a single link in the branch is only 512 kbps, which does not meet requirements. As a result, the high-definition video conference cannot be held smoothly, and severe pixelation occurs in video images.

The multilink bundling function establishes virtual WAN channels and virtual links between devices in the headquarters and branch. It bundles the bandwidth of two links so that data flows of the branch overcome the 512 kbps restriction of a single link, and transmits data flows at the bandwidth of the two links, that is, 1 Mbps, thereby ensuring smooth high-definition video conference.

Figure 1-1



Remarks	The pipes in light green indicate VWAN channels. Arrow lines in blue and orange indicate virtual links.

Deployment

Enable multilink bundling on both devices in the headquarters and branches.

Configure VWAN channels on both devices in the headquarters and branches.

Configure virtual links on both devices in the headquarters and branches so that links of the same ISP are used to establish a virtual link, to prevent cross-ISP network transmission.

Configure server addresses of key services on the device in the headquarters.

Configure an ACL on the device in the branch, to perform multilink bundling on data flows of only some users accessing servers.

1.3 Features

Basic Concepts

VWAN Channel

A VWAN channel can be configured separately. As an abstract unit, a VWAN channel is used to manage and configure multiple bundled links in a unified manner. A VWAN channel, based on link bandwidth, schedules different virtual links in polling mode during data transmission. MP is used to encapsulate and send the packets, to ensure load balancing of links and full aggregation of bandwidth. A VWAN channel is identified by name. The same name needs to be configured at both ends of one VWAN channel to facilitate verification.
VWAN channels are classified into VWAN channels in passive mode and VWAN channels in active mode. VWAN channels in passive mode are applicable to the device in the headquarters. The device passively waits for the access of devices in branches, and dynamically creates VWAN channels. Therefore, only one VWAN channel in passive mode is required in the headquarters, to implement multilink bundling between the devices in the headquarters and different branches, thereby simplifying user configuration. VWAN channels in active mode are applicable to devices in branches. The devices actively establish connections with the device in the headquarters.

➘ Virtual Link

A virtual link maps to actual physical links. A virtual link is identified by the device port at the local end of the link and peer IP address. It utilizes the MP (based on the User Datagram Protocol (UDP)) to implement the negotiation and connection, disconnection, data encapsulation, and link keepalive functions.
Based on the type of VWAN channels to which virtual links belong, virtual links are also classified into virtual links in passive mode and virtual links in active mode. A virtual link in passive mode specifies the local device port but does not restrict the peer the IP address; a virtual link can be still established successfully when the IP address of an ADSL link in the branch is changed. The local device listens to the virtual link in passive mode and wait for the peer device to initiate negotiation to establish a connection. After the local device port and peer IP address are specified, a virtual link in active mode actively constructs handshake packets and initiates negotiation to establish a connection.

➘ ACL

- An ACL is used to match data flows based on the source IP address, destination IP address, transport-layer protocol, and transport-layer port ID in IP packets. An ACL can be configured for VWAN channels in active mode, to conduct multilink bundling on data flows of only some users accessing servers.

Overview

Feature	Description
Multilink Bundling	Establishes VWAN channels and virtual links between devices in the headquarters and branches of an enterprise, and specifies data flows that come from branches for access to servers in the headquarters for multilink bundling, so as to overcome the bandwidth restriction of a single link and aggregate the bandwidth of multiple physical links.

1.3.1 Multilink Bundling

Multilink bundling establishes VWAN channels and virtual links between devices in the headquarters and branches of an enterprise, and specifies data flows that come from branches for access to servers in the headquarters for multilink bundling, so as to overcome the bandwidth restriction of a single link and aggregate the bandwidth of multiple physical links.

Working Principle

Multilink bundling is mainly used in scenarios in which the enterprise headquarters use high-bandwidth and high-quality links (such as fiber links) whereas branches use multiple low-bandwidth links (such as ADSL dialup links) to access the WAN. Key applications between devices in the headquarters and branches, such as applications related to heavy traffic transmission and real-time video conference, are restricted by the bandwidth of a single link. They may encounter low transmission rate, low video resolution, severe pixilation, and other

problems. Multilink bundling establishes VWAN channels and virtual links between devices in the headquarters and branches of an enterprise. A VWAN channel, based on the link bandwidth, schedules different virtual links in polling mode, and encapsulates and sends packets via MP, so as to ensure load balancing of links and full aggregation of bandwidth. Data flows of key applications of the enterprise can be transmitted at a rate approximate to the total bandwidth of multiple links.

Establishing VWAN Channel

A VWAN channel in passive mode is configured on the device in the enterprise headquarters, and a VWAN channel in active mode is configured on the device in a branch. The same name should be configured at both ends of a VWAN channel for identification and verification, to prevent an establishment failure or incorrect access. VWAN channels in active mode can be commented with branch names for identification on the device in the headquarters.

Based on the status of bundled virtual links, a VWAN channel can be in the closed, opened, or established state.

Closed state: No virtual link is configured.

Opened state: A virtual link is configured but the virtual link is not established successfully.

Established state: A virtual link is established successfully.

Establishing Virtual Link

A virtual link in passive mode is configured on the device in the enterprise headquarters, and a virtual link in active mode is configured on the device in a branch. After configuration, a virtual link in active mode actively constructs handshake packets (SYN/SSYN packets) to initiate negotiation to establish a connection. The local device listens to the virtual link in passive mode and wait for the peer device to initiate negotiation to establish a connection. After a virtual link is established successfully, data packets are encapsulated and sent, and keepalive packets (ping/pong packets) are used to detect link faults. A virtual link uses RST packets to interrupt a connection.

A virtual link has the following states:

Free state: Multilink bundling is disabled, the local device port of the virtual link is in the down state, or no master IP address is configured.

Connecting state: A virtual link is being negotiated.

Established state: A virtual link is established successfully.

Fault state: A virtual link does not receive data packets or keepalive packets within 5 seconds. A virtual link in the fault state does not participate in the polling scheduling of the VWAN channel, to prevent loss of data packets.

Closing state: A virtual link is being disconnected.

Listen state: The local device listens to the virtual link in passive mode and wait for the peer device to initiate negotiation to establish a connection.

Specifying Data Flow

A VWAN channel needs to specify data flows that need to be transmitted through the VWAN channel for multilink bundling. The device in the headquarters is enabled to push server addresses to specify such data flows, that is, server addresses need to be configured for the VWAN channel in passive mode. After a VWAN channel is established successfully, the VWAN channel in passive mode pushes server addresses to the peer device for data flow matching. Server addresses do not need to be configured for the VWAN channel in active mode, simplifying user configuration.

If multilink bundling is required for data flows of only some users in the branch accessing servers, an ACL can be associated with the VWAN channel in active mode to restrict data flows.

Related Configuration

Enabling Multilink Bundling

By default, multilink bundling is disabled.

Run the **vwan channel enable** command to enable the multilink bundling function.

A virtual link can be negotiated and established only after multilink bundling is enabled.

Configuring VWAN Channel

By default, no VWAN channel is configured.

Run the **vwan channel [passive | active]** *channel-name* command to configure a VWAN channel. VWAN channels are classified into VWAN channels in passive mode and VWAN channels in active mode.

After a VWAN channel is configured successfully, you can configure virtual links, server addresses, and other functions in VWAN channel configuration mode.

Configuring Virtual Link

By default, no virtual link is configured.

In configuration mode of a VWAN channel in passive mode, run the **link** *interface-name* [*source-port*] **any** command to configure a virtual link in passive mode. In configuration mode of a VWAN channel in active mode, run the **link** *interface-name* [*source-port*] *dest-ip* [*dest-port*] [**bandwidth** *bandwidth*] command to configure a virtual link in active mode.

If multilink bundling is enabled, a master IP address is configured for a port, and the port is in the Up state, the virtual link in passive mode switches to the listen state, the virtual link in active mode switches to the connecting state, and the peer device actively initiates negotiation to establish a connection.

Configuring Server Address

By default, no server address is configured.

In configuration mode of a VWAN channel in passive mode, run the **server** *server-ip* **[tcp** *tcp-port* **| udp** *udp-port* **]** command to configure a server address.

If a VWAN channel is in the established state, the VWAN channel in passive mode pushes server addresses to the peer device.

Associating ACL

By default, no ACL is associated.

In configuration mode of a VWAN channel in active mode, run the **access-list** *acl-num* command to associate an ACL.

After an ACL is associated, data flows of some users accessing servers can be restricted to not enter a VWAN channel for multilink bundling.

Commenting VWAN Channel with Branch Name

By default, no branch name is commented.

In configuration mode of a VWAN channel in active mode, run the **comment** *name* command to comment the VWAN channel with a branch name.

If a VWAN channel is in the established state, the local device advertises the local name to the peer device through the VWAN channel in active mode.

Restricting Number of Channels That Can Be Created in VWAN Channel in Passive Mode

By default, the number of channels that can be created in a VWAN channel in passive mode is restricted to the maximum number of VWAN channels supported by the device.

In configuration mode of a VWAN channel in passive mode, run the **limit** *channel-num* command to restrict the number of channels that can be created in the VWAN channel in passive mode.

If the number of channels dynamically created in a VWAN channel in passive mode exceeds the specified quantity, no more devices in branches are allowed to access.

1.4 Configuration

SG-5110 products do not support channel acceleration.

Configuration	Description and Command	
Configuring Multilink Bundling	(Mandatory) It is used to establish VWAN channels and virtual links, and specify data flows that require multilink bundling. Multilink bundling is used only in gateway mode. Default routes need to be configured for ports of virtual links.	
	vwan enable	Enables multilink bundling.
	vwan channel [**passive** | **active**] *channel-name*	Configures a VWAN channel.
	link *interface-name* [*source-port*] **any**	Configures a virtual link in passive mode.
	link *interface-name* [*source-port*] *dest-ip* [*dest-port*] [**bandwidth** *bandwidth*]	Configures a virtual link in active mode.
	server *server-ip* [**tcp** *tcp-port* | **udp** *udp-port*]	Configures a server address.
	(Optional) It is used to configure advanced functions such as associating an ACL, commenting a VWAN channel with a branch name, restricting the channel quantity, and changing the value of the MSS field.	
	access-list *acl-num*	Associates an ACL, so that multilink bundling is not performed on data flows of some users in the branch who access servers.
	comment *name*	Comments a VWAN channel with a branch name.
	limit *channel-num*	Restricts the number of channels that can be created in a VWAN channel in passive mode.
	vwan mss *mss-val*	Changes the value of the TCP MSS field to a specified value.

1.4.1 Configuring Multilink Bundling

Configuration Effect

Establish VWAN channels and virtual links successfully, and enable the VWAN channels and virtual links to be in the established state. Enable the VWAN channel in a branch to receive server addresses pushed by the device in the headquarters.

Notes

Multilink bundling is used only in gateway mode.

Configuration Steps

Enabling Multilink Bundling

Mandatory.
Perform the configuration on both devices in the headquarters and branches.

Configuring VWAN Channel

Mandatory.
Configure a VWAN channel in passive mode on the device in the enterprise headquarters, and configure a VWAN channel in active mode on the device in the branch.

Configuring Virtual Link

Mandatory.
Configure a virtual link in passive mode on the device in the enterprise headquarters, and configure a virtual link in active mode on the device in the branch.
Configure default routes for ports of links to be configured. If a routing mode of a higher priority such as route database-based routing affects the default routing, a virtual link may fail to be established.

Configuring Server Address

Mandatory.
Configure an internal server address on the device in the headquarters.

Associating ACL

Optional. Configure an ACL when multilink bundling is not required for data flows of some users in the branch who access servers in the headquarters.
Configure an ACL on the device in the branch, so that VWAN channels are not configured and multilink bundling is not performed on data flows of some users accessing servers.

Commenting VWAN Channel with Branch Name

Optional. When devices in multiple branches are connected to the device in the headquarters, comment VWAN channels of the branches with branch names so that they are identified by the device in the headquarters.
Perform the configuration on devices in branches to facilitate identification by the device in the headquarters.

Restricting Number of Channels That Can Be Created in VWAN Channel in Passive Mode

Optional. When multiple VWAN channels in passive are configured on the device in the headquarters, you can configure the number of channels that can be created in each VWAN channel in passive mode.
Perform the configuration on the device in the headquarters, to restrict the number of channels that can be created in a VWAN channel in passive mode.

Changing Value of TCP MSS Field

Optional. When the maximum transmission unit (MTU) of a physical link is not the default 1500 bytes, the MSS field can be set, to prevent IP fragmentation caused because the length of TCP packets exceeds the link MTU.

Perform the configuration on both devices in the enterprise headquarters and branches, to prevent fragmentation of a large number of IP packets caused because the length of TCP packets encapsulated via MP or FEC exceeds the link MTU.

Verification

Check whether VWAN channels and virtual links are successfully established.
Check whether the device in the branch receives server addresses pushed by the device in the headquarters.
Use a PC in the branch to access the video server and OA server in the headquarters. Check whether data flows are normally transmitted via the VWAN channels.

Related Commands

Enabling Multilink Bundling

Command	**vwan channel enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring VWAN Channel

Command	**vwan channel** [**passive** | **active**] *channel-name*
Parameter Description	**passive**: Configures a VWAN channel in passive mode. **active**: Configures a VWAN channel in active mode. *channel-name*: Indicates the name of a VWAN channel. The name contains a maximum of 31 characters.
Command Mode	Global configuration mode
Usage Guide	VWAN channels in passive mode are applicable to the device in the headquarters while VWAN channels in active mode are applicable to the device in branches. Ensure that names at both ends of a VWAN channel are consistent.

Configuring Virtual Link in Passive Mode

Command	**link** *interface-name* [*source-port*] **any**
Parameter Description	*interface-name*: Indicates the device port at the local end of a virtual link. *source-port*: Indicates the UDP source port used by MP. It does not need to be configured. The default value is Port 12315.
Command Mode	Configuration mode of a VWAN channel in passive mode
Usage Guide	When the master IP address has been configured for a specified device port and the device port is in the Up state, the virtual link in passive mode switches to the listen state and the local device waits for the peer device to initiate a connection.

Configuring Virtual Link in Active Mode

Command	**link** *interface-name* [*source-port*] *dest-ip* [*dest-port*] [**bandwidth** *bandwidth*]
Parameter Description	*interface-name*: Indicates the device port at the local end of a virtual link. *source-port*: Indicates the UDP source port used by MP. It does not need to be configured. The default value is Port 12315. *dest-ip*: Indicates the peer IP address of a virtual link, that is, the master IP address of the peer device port. *dest -port*: Indicates the UDP destination port used by MP. It does not need to be configured. The default value is Port 12315. **bandwidth** *bandwidth*: Indicates the link bandwidth (unit: kbps). It does not need to be configured. By default, it is the same as the bandwidth configured in interface configuration mode.
Command Mode	Configuration mode of a VWAN channel in active mode
Usage Guide	When the master IP address has been configured for a specified device port and the device port is in the Up state, the virtual link in active mode switches to the connecting state and the peer device actively initiates a connection. If Port 12315 is disabled, specify another port. In a VWAN channel, a virtual link is scheduled in polling mode based on the configured link bandwidth for packet transmission. Therefore, the configured link bandwidth needs to be consistent with the actual physical link bandwidth, to ensure load balancing among multiple virtual links and optimal bandwidth aggregation effect.

Configuring Server Address

Command	**server** *server-ip* [**tcp** *tcp-port* | **udp** *udp-port*]
Parameter Description	*server-ip*: Indicates the IP address of a server. It is usually set to the IP address after NAT static mapping or port mapping is performed. **tcp** *tcp-port*: Indicates the port ID of the server TCP application. **udp** *udp-port*: Indicates the port ID of the server UDP application.
Command Mode	Configuration mode of a VWAN channel in passive mode
Usage Guide	The TCP port and UDP port do not need to be configured. You can run the **ping** command to detect the connectivity between PCs in the branch and the servers. When services that do not need multilink bundling exist on a server, you can specify the TCP port or UDP port. A maximum of 128 server addresses can be configured.

Associating ACL

Command	**access-list** *acl-num*
Parameter Description	*acl-num*: Indicates the serial number of the ACL to be associated.
Command Mode	Configuration mode of a VWAN channel in active mode
Usage Guide	An ACL does not need to be configured. The ACL is used to so that multilink bundling is not performed on data flows

	of some users in the branch who access servers.

Commenting VWAN Channel with Branch Name

Command	**comment** *name*
Parameter Description	*name*: Indicates the name of a branch. It contains a maximum of 31 characters.
Command Mode	Configuration mode of a VWAN channel in active mode
Usage Guide	After a VWAN channel is established successfully, the device in the branch advertises its branch name through the VWAN channel in active mode to the peer device for identification.

Restricting Number of Channels That Can Be Configured in VWAN Channel in Passive Mode

Command	**limit** *channel-num*
Parameter Description	*channel-num*: Indicates the number of channels that can be created in a VWAN channel in passive mode. The default value is the maximum number of VWAN channels supported by the device.
Command Mode	Configuration mode of a VWAN channel in passive mode
Usage Guide	It does not need to be configured.

Changing Value of TCP MSS Field

Command	**vwan mss** *mss-val*
Parameter Description	*mss-val*: Indicates the value of the MSS field. If the value of the MSS field in TCP SYN packets is greater than the value, change the value of the MSS field. The value ranges from 500 to 1,460.
Command Mode	Global configuration mode
Usage Guide	It does not need to be configured. During MP encapsulation and FEC encapsulation, bytes added during encapsulation are automatically removed from the value of the MSS field.

Displaying Information About VWAN Channel

Command	**show vwan channel**
Parameter Description	*N/A*
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	Display information about a VWAN channel, such as the status and name of the VWAN channel, peer branch name, serial number of the associated ACL, and number of transmitted and received packets. The status shows whether the VWAN channel is successfully established.

Displaying Information About Virtual Link

Command	**show vwan link**
Parameter Description	*N/A*
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	Display information about a virtual link, such as the status and bandwidth of the virtual link, local port ID, IP addresses and UDP ports of the local and peer devices, and number of transmitted and received packets. The status shows whether the virtual link is successfully established.

Displaying List of Server Addresses Pushed by Peer Device

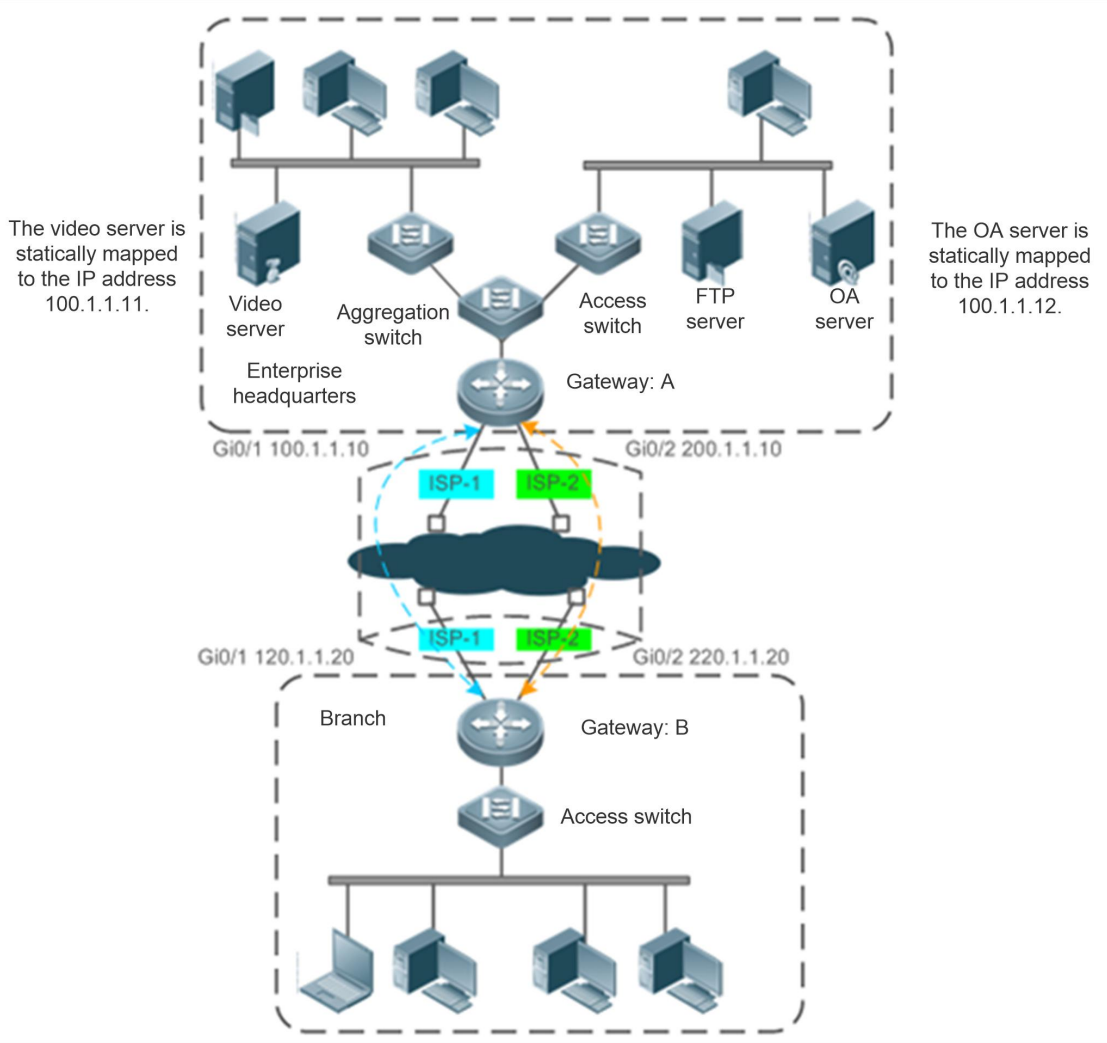
Command	**show vwan channel servers**
Parameter Description	*N/A*
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	Use this command on the device in a branch to display the list of server addresses pushed by the device in the headquarters.

Displaying Traffic Information About VWAN Channel

Command	**show vwan flowrate** [cha*nnel-id*]
Parameter Description	*channel-id*: Indicates the ID of a VWAN channel. If no VWAN channel is specified, information about accumulated traffic of all VWAN channels is displayed.
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	Display traffic information about a VWAN channel, so as to check data flows of users in a branch who access servers in the headquarters are successfully transmitted via the VWAN channel.

Configuration Example

Configuring Multilink Bundling

Scenario Figure 1-2	
Configuration Steps	● Enable multilink bundling on the device in the headquarters, configure a VWAN channel in passive mode, and set the channel name to CompanyA. ● On the device in the headquarters, use Port Gi0/1 and Port Gi0/2 to configure virtual links in passive mode and wait for the device in the branch to initiate negotiation to establish connections. ● Configure NAT static mapping for the video server and OA server in the headquarters, and map the video server and OA server to 100.1.1.11 and 100.1.1.12 respectively (omitted). ● On the device in the headquarters, configure server addresses to the IP addresses of the video server and OA server that are statically mapped. ● On the device in the branch, enable multilink bundling, configure a VWAN channel in active mode, and set the channel name to CompanyA. ● On the device in the branch, use Port Gi0/1 and Port Gi0/2 to configure virtual links in active mode to establish connections with the device in the headquarters. ● Configure bandwidth for ports on the device in the branch (omitted). ● Comment the VWAN channel with the branch name on the device in the branch to facilitate identification by the device in the headquarters.
Headquarters	Headquarters # configure terminal

Gateway A	Headquarters (config)# vwan channel enable Headquarters (config)# vwan channel passive CompanyA Headquarters (config-vwan-channel)# link GigabitEthernet 0/1 any Headquarters (config-vwan-channel)# link GigabitEthernet 0/2 any Headquarters (config-vwan-channel)# server 100.1.1.11 Headquarters (config-vwan-channel)# server 100.1.1.12
Branch Gateway B	Branch # configure terminal Branch (config)# vwan enable Branch (config)# vwan channel active CompanyA Branch (config-vwan-channel)# link GigabitEthernet 0/1 100.1.1.10 Branch (config-vwan-channel)# link GigabitEthernet 0/2 200.1.1.10 Branch (config-vwan-channel)# comment BranchA
Verification	● Check whether VWAN channels and virtual links are successfully established. ● Check the device in the branch receives server addresses pushed by the device in the headquarters. ● Use a PC in the branch to access the video server and OA server in the headquarters. Check whether data flows are normally transmitted via the VWAN channels.
Headquarters Gateway A	Headquarters # show vwan channel Headquarters # show vwan link Headquarters # show vwan flowrate
Branch Gateway B	Branch # show vwan channel Branch # show vwan link Branch # show vwan channel servers Branch # show vwan flowrate

Common Errors

Names configured at both ends of a VWAN channel are inconsistent.

1.5 Monitoring

Displaying

Description	Command
Displays information about a VWAN channel.	**show vwan channel**
Displays information about a virtual link.	**show vwan link**
Displays the list of server addresses pushed by the peer device.	**show vwan channel servers**
Displays traffic information about a VWAN channel.	**show vwan flowrate**

2 Configuring HT TP-AD

2.1 Overview

HTTP-AD is a feature that inserts ads into mobile Web pages. With this feature, you can insert a designated ad script into the source file of an HTTP-based Hypertext Markup Language (HTML) Web page for operation purposes.

2.2 Applications

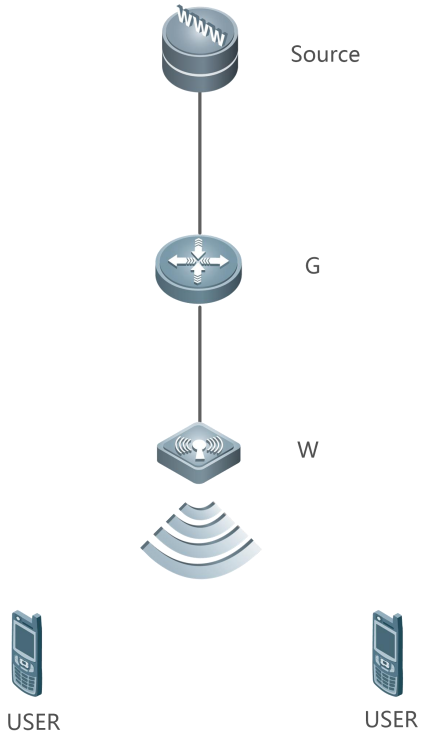
Application	Description
Applying HTTP-AD	A mobile phone accesses an HTML Web page via a gateway.

2.2.1 Applying HTTP-AD

Scenario

A mobile phone accesses an HTML Web page via a gateway.

As shown in Figure 2-1, a mobile phone connects to a wireless access point (AP) and then accesses an HTML Web page via a gateway. The gateway serves as a proxy to process Hypertext Transfer Protocol (HTTP) packets and insert ad scripts. Finally, an inserted ad pops up on the Web page.



Remarks	G is an egress gateway. W is a wireless AP that provides network connections for the mobile phone. Source is an HTTP server.

Deployment

- Enable the acceleration function on the gateway.
- Enable the moving ad function on the gateway.

2.3 Features

Basic Concepts

➘ Port-based TCP Proxy

The gateway serves as a proxy to process specific TCP streams, and in addition, process HTTP streams in the moving ad cache scenario. The default HTTP port is Port 80.

➘ Ad Script Insertion

The ad script insertion function can insert operator-defined ads into web pages browsed by the user on the mobile phone.

Overview

Feature	Description
Moving Ads	Pops up ads on HTML Web pages browsed by the user on the mobile phone.
HTTP Packet Processing by Using Proxy	Processes specific TCP streams by using a proxy.

2.3.1 Moving Ads

Working Principle

A mobile phone displays Web pages based on the HTTP. For HTML Web pages, packets are processed by using a proxy, and ad scripts are inserted into response packets, so that ads can be displayed on the Web pages browsed by the user.

Content in the ad script determines the display effect. Ads cannot be inserted into non-HTML Web pages, and no ad script is inserted into non-HTTP (for example, HTTPS) packets.

Related Configuration

Configuring Enabling Switch

No enabling switch is configured by default.

Run the **was enable** command to enable the WAS module.

Run the **was http ad enable** command to enable the moving ad function.

Configuring Enabling Switch

Run the **was http ad url** *stirng* command to configure the ad script link.

2.3.2 HTTP Packet Processing by Using Proxy

Working Principle

The TCP proxy function sends packets to the user space for processing and then forwards the packets. A specific port is configured and packets on this port are processed by using the TCP proxy. The default HTTP port is Port 80.

Related Configuration

Configuring TCP Proxy Rules

No TCP proxy rule is configured by default.

2.4 Configuration

Configuration	Description and Command	
Enabling Moving Ad Function	(Mandatory) It is used to enable the moving ad function in global configuration mode.	
	was enable	Enables the WAS module in global configuration mode.

	was http ad enable	Enables the moving ad function.
Configuring Proxy for HTTP Streams	(Mandatory) It is used to configure a proxy for HTTP **Streams**.	
	in-path rule auto-discovery dstport port 80 accelerate http rulenum start	Configures the TCP proxy rule, that is, configures Port 80 for HTTP packets.

2.4.1 Enabling Moving Ad Function

Configuration Effect

- Enable the WAS module in global configuration mode.
- Enable HTTP-AD in global configuration mode.
- Configure the URL of an ad script.

Notes

- When enabling the WAS module, you will be prompted to restart the device because the flow table modification is involved.

Configuration Steps

Enabling was Module in Global Configuration Mode

- Mandatory. If the WAS module is not enabled, moving ads cannot be displayed.

Command	**was enable**
Parameter Description	N/A
Defaults	The WAS module is disabled.
Command Mode	Global configuration mode
Usage Guide	The WAS module must be enabled to provide the moving ad function.

Enabling Moving Ad Function

- Mandatory. Moving ads cannot be displayed if the moving ad function is disabled.

Command	**was http ad enable**
Parameter Description	N/A
Defaults	The moving ad function is disabled.
Command Mode	Global configuration mode
Usage Guide	This command is used to enable the moving ad function.

Verification

- Run the show **was status** command to check whether the WAS module is enabled.

Command	**show was status**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	Check whether the WAS module is enabled.
Command Presentation	FS(config)#show was status **was:on**

- Run the **show was http ad config** command to check the configuration of the moving ad function.

Command	**show was http ad config**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	Check the configuration of the moving ad function.
Command Presentation	FS(config)#show was http ad config **ad status : on** ad url : http://fs.com

Configuration Example

Enabling HTTP-AD

Configuration Steps	- Enable HTTP-AD on the gateway.
	FS# configure terminal FS(config)# was enable FS(config)# was http ad enable FS(config)# was http ad url http://fs.com
Verification	- Run the **show was http ad config** command to check whether HTTP-AD is enabled. FS# svr(config)#sh was status was: on FS#show was http ad config ad status : on ad url : http://fs.com

2.4.2 Configuring Proxy for HTTP Streams

Configuration Effect

- Port 80-based HTTP steams are processed by using a proxy.

Configuration Steps

Configuring Port 80-based TCP Proxy Rule

- Mandatory. Moving ads cannot be properly displayed if no TCP proxy is configured.

Command	**in-path rule auto-discovery dstport port 80 accelerate http rulenum start**
Parameter Description	N/A
Defaults	No TCP proxy is configured.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure a TCP proxy.

Verification

- Run **the** show **in-path rules** command to check whether the Port 80-based TCP proxy rule is configured.

Command	**show in-path rules**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	Check whether the WAS module is enabled.
Command Presentation	FS#show in-path rules Rule Type O VLAN App Source Addr/Mask Source port Dest Addr/Mask Dest port description 1 auto N all http all port:all all port:80 def pass N all none all port:all all port:all any (O) Optimization Policy: F=Full D=DRE-only C=Compression-only M=DRE-M N=None

Configuration Example

Configuring Proxy for HTTP Streams

Configuration Steps	• Configure the Port 80-based TCP proxy rule.
	FS# configure terminal FS(config)# in-path rule auto-discovery dstport port 80 description http80 accelerate http

Verification	● Check the TCP proxy rule. FS# show in-path rule Rule Type O VLAN App Source Addr/Mask Source port Dest Addr/Mask Dest port description 1 pass N all none all port:all all name:Secure Secure(bypass) 2 pass N all none all port:all all name:Interactive Interactive(bypass) 3 auto N all http all port:all all port:all http 4 auto N all http all port:all all port:80 http80 def pass N all none all port:all all port:all any

2.5 Monitoring

Displaying

Description	Command
Displays the configuration of the moving ad function.	**show was http ad config**
Displays the current status of the moving ad function.	**show was http ad status**
Displays the TCP proxy rule.	**show in-path rule**

3 Configuring APP-CACHE

3.1 Overview

APP-CACHE is a function module used to cache downloaded mobile phone apps. It can cache all Android and Apple app files, or cache only app files from a specific provider.

Protocols and Standards

- N/A

3.2 Applications

Application	Description
Applying APP-CACHE	A mobile phone downloads files from the file server via the gateway.

3.2.1 Applying APP-CACHE

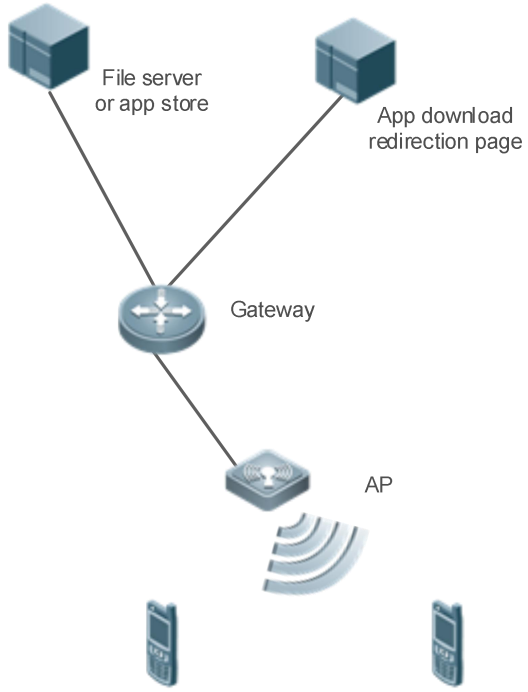
Scenario

As shown in Figure 3-1, in commercial Wi-Fi scenarios, a mobile phone user usually needs to download a specific app in order to perform Wi-Fi application authentication. The gateway caches the downloaded app installation file, which increases the download speed and improves user experience.

The original app file is stored in the file server. After a mobile phone user downloads and installs the app file, other users can obtain the file directly from the gateway.

A mobile phone user first accesses the download page, which is then redirected to the file server for downloading. With the APP-CACHE feature, the gateway can cache specified app files.

Figure 3-1



Deployment

- Enable the acceleration function on the gateway.
- Enable APP-CACHE on the gateway.
- Configure the domain name of the file server or app store.
- Configure the URL of the app download redirection page.

3.3 Features

Basic Concepts

Domain Name-based TCP Proxy

The domain name-based TCP proxy processes TCP streams that are used for caching app files, and processes Hypertext Transfer Protocol (HTTP) streams of specific servers in the app file cache scenario. The domain name-based TCP proxy parses out the server address according to the configured domain name and URL, and processes HTTP sessions for accessing the server.

App File Cache

The gateway caches the app package files downloaded by mobile phone users. With the cache function, app files can be directly obtained from the local gateway when users initiate repeated download requests. Currently, most common app files are Android APK files and Apple IPA files.

Designated App File Cache

In free Wi-Fi scenarios, the gateway caches only app files designated by the customer, and does not accelerate the download of other non-designated app files.

Features

Feature	Description
Domain Name-based TCP Proxy	Processes specific TCP streams.
App File Cache	Caches app files.
Caching of Designated App Files	Caches designated app files only.

3.3.1 Domain Name-based TCP Proxy

Working Principle

The TCP proxy function sends packets to the user space for processing and then forwards the packets. With the domain name or IP address of the app file cache server configured, some specific streams for accessing the server can be processed by the TCP proxy.

Related Configuration

Configuring a Domain Name

No domain name is configured by default.

Run the **was http inpath domain** *string* command to specify the domain name of the server for which a proxy is configured.

3.3.2 App File Cache

Working Principle

A mobile phone downloads an app file over HTTP. During the first download, if the APP-CACHE module identifies an APK or IPA download link in the URL, it caches the response packet. When another mobile phone downloads the same app file next time, the request packet hits the cache, and the gateway directly constructs and returns a response packet to the mobile phone.

Related Configuration

Enabling Functions

The functions are disabled by default.

Run the **was enable** command to enable the WAS module.

Run the **was http app-cache enable** command to enable the APP-CACHE function of the WAS module.

3.3.3 Caching of Designated App Files

Working Principle

When downloading an app file, a mobile phone user usually accesses an direction page (such as a portal page) of the app provider, and then click the corresponding mobile phone operating system to access the file server or app store for download. Based on this, a 10-minute window time is set. If a mobile phone user accesses the URL of the designated app, the IP address of the mobile phone is recorded. The gateway caches IPA or APK file requested from this IP address within 10 minutes, and does not process requests initiated after 10 minutes.

If the user behavior does not comply with the behavior prediction, the gateway may incorrectly cache other app files or not cache any app file. In this case, the cache function is invalid, which is imperceptible to users.

Related Configuration

Caching Designated App Files

No app file is designated by default. In this case, the gateway caches all app files.

Run the **was http app-cache url** *string* command to configure the URL of the app file download page.

3.4 Configuration

Configuration	Description and Command	
Enabling APP-CACHE	(Mandatory) It is used to enable the APP-CACHE function globally.	
	was enable	Enables the WAS module globally.
	was http app-cache enable	Enables APP-CACHE.
Configuring the Domain Name or IP Address of the File Download Server	(Mandatory) It is used to designate a file server and configure a TCP proxy for packets of the file server.	
	was http inpath domain *string*	Configures the domain name of the file server.
Configuring the App File Matching Rule	(Optional) It is used to modify the cache matching rule.	
	was http app-cache rule type *string*	Configures the file type for matching.
	was http app-cache rule key *string*	Configures the URL matching algorithm.
Caching Designated App Files	(Optional) It is used to cache only designated app files.	
	was http app-cache url *string*	Configures the URL of the app download page.

3.4.1 Enabling APP-CACHE

Configuration Effect

- Enable the WAS module globally.
- Enable APP-CACHE globally.

Notes

- When enabling the WAS module, you will be prompted to restart the device because the flow table modification is involved.

Configuration Steps

- Mandatory.

Verification

- Check that the TCP streams are successfully transmitted to the WAS module of the gateway proxy.

Related Commands

Enabling the WAS Module

Command	was enable
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	

Enabling APP-CACHE

Command	was http app-cache enable
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Enable APP-CACHE.

Configuration Example

Enabling APP-CACHE

Configuration Steps	● Enable APP-CACHE on the gateway.
	FS# configure terminal FS(config)# was enable FS(config)# was http app-cache enable
Verification	● Run the **show was http app-cache config** command to check whether APP-CACHE is enabled. FS# svr(config)#sh was status was: on FS (config)#show was http app-cache config app-cache : on

3.4.2 Configuring the Domain Name or IP Address of the File Download Server

Configuration Effect

- Use the gateway proxy to process HTTP streams for accessing the download server.

Notes

- Make sure that the DNS server is correctly configured before you configure the domain name.

Configuration Steps

- Mandatory.

Verification

- Check that the HTTP streams for accessing the designated domain name are successfully transmitted to the gateway proxy.

Related Commands

Configuring the Domain Name or IP Address of the File Download Server

Command	**was http inpath domain** *string*
Parameter Description	*string*: Indicates the domain name or IP address.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the download server for APP-CACHE.

Configuration Example

Configuring the Domain Name of the File Download Server

Configuration Steps	Configure the file download server according to the domain name.
	FS# configure terminal FS(config)# was http inpath domain itunes.apple.com
Verification	Verify that an APK file downloaded from http://www.FS.com can be cached. FS#show was http inpath domain inpath domain: www.FS.com 70.39.84.230

Configuring the IP Address of the File Server

Configuration Steps	Configure the file server according to the IP address.
	FS# configure terminal FS(config)# was http inpath domain 10.0.0.10
Verification	Verify that an IPA or APK app file downloaded over HTTP from http://www.FS.com can be cached.
	FS#show was http inpath domain inpath domain: 10.0.0.10 10.0.0.10

3.4.3 Configuring the App File Type Matching Rule

Configuration Effect

- Determine the type of files to be cached or URL matching algorithm by configuring the matching rule.

Configuration Steps

- Optional.
- Cache files according to the designated rule.

Verification

- Check that the configured rule takes effect.

Related Commands

Configuring the File Type

Command	**was http app-cache rule type** *string*
Parameter Description	*string*: Indicates the file type.
Command Mode	Global configuration mode
Usage Guide	Configure the file type according to the type of files to be cached.

Configuring URL Authentication

Command	**was http app-cache rule key** *string*
Parameter Description	*string*: Indicates the matching algorithm.
Configuration Mode	Global configuration mode
Usage Guide	Combine $host, $path, $name, and $args, which respectively correspond to the elements in the URL.

Configuration Example

Configuring the Caching of .exe Files

Configuration Steps	Configure the cache function to support cache of .exe files.
	FS# configure terminal FS(config)# was http app-cache rule type exe FS(config)# end
Verification	Verify that a downloaded .exe file can be cached.

Configuring the URL Matching Algorithm to Match a Specific Host and File Name

Configuration Steps	Configure a specific host and a file name.
	FS# configure terminal FS(config)# was http app-cache rule key $host$name
Verification	Verify that only files of the specific host are cached.

3.4.4 Caching Designated App Files Based on the Time Window

Configuration Effect

- Cache designated app files only.

Notes

The algorithm is based on the user behavior prediction.

Configuration Steps

- Optional.
- Designate the to-be-cached app file by configuring the download redirection page of the app provider.

Verification

- Verify that only the app file downloaded within 10 minutes after access to the redirection page is cached.

Related Commands

Configuring the URL of the App Download Page

Command	**was http app-cache url** *string*
Parameter Description	*string:* Indicates the URL of the app download page.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Authentication-free IP Address Range

Configuration Steps	• Configure the URL of the app download page.
	FS (config)# was http app-cache url http://fs.com

Verification	● Run the **show was http app-cache config** command to check the configuration. FS#show was http app-cache config app-cache url num 1: 0 http://fs.com ● Simulate the app download operation and check the cache status.

3.4.5 Caching Designated App Files Based on the URL Characteristic String

Configuration Effect

- Cache designated app files only.

Configuration Steps

- Optional.
- Designate the to-be-cached app file by configuring the URL characteristic string.

Verification

- Verify that only the app file downloaded from the designated URL can be cached.

Related Commands

Configuring the URL Characteristic String of the App Download Page

Command	**was http app-cache match url** *string*
Parameter Description	*string:* Indicates the characteristic string of the file URL.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Authentication-free IP Address Range

Configuration Steps	● Configure the URL characteristic string of the app download page.
	FS (config)# was http app-cache match url FS
Verification	● Run the **show was http app-cache config** command to check the configuration. ● Simulate the app download operation and check the cache status.

3.4.6 Caching Designated App Files Based on the App Name

Configuration Effect

- Cache designated app files only.

Configuration Steps

- Optional.
- Designate the to-be-cached app file by configuring the app name.

Verification

- Verify that only the file of the designated app name can be cached.

Related Commands

Configuring the App Name of the App Download Page

Command	**was http app-cache app-name** *string*
Parameter Description	*string:* Indicates the app name.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Authentication-free IP Address Range

Configuration Steps	● Configuring the app name of the app Download Page
	FS (config)# was http app-cache match app-name testapp
Verification	● Run the **show was http app-cache config** command to check the configuration. FS#show was http app-cache config

	● Simulate the app download operation and check the cache status.

3.5 Monitoring

Displaying

Description	Command
Displays the configuration.	**show was http app-cache config**
Displays the current status.	**show was http app-cache status**
Displays multi-threading download status.	**Show was http app-cache muldownload status**
Displays the file cache database.	**show was http app-cache database**
Displays the domain name configuration.	**show was http inpath domain**

Chapter 2 Application Configuration

1. Configuring Network Communication Test Tools
2. Configuring DHCP
3. Configuring DNS
4. Configuring DDNS
5. Configuring NTP
6. Configuring SNTP
7. Configuring DNS Proxy
8. Configuring FTP Server
9. Configuring Time Range
10. Configuring Smart-DNS

1 Configuring Network Communication Test Tools

1.1 Overview

Network communication test tools can be used to check the connectivity of a network and helps you analyze and locate network faults. Network communication test tools include Packet Internet Groper (PING) and Traceroute. Ping is used to check the connectivity and delay of a network. A greater delay indicates a slower network speed. Traceroute helps you learn about the topology of physical and logical links and transmission rate. On a network device, you can run the ping and traceroute commands to use the two tools respectively.

Protocols and Standards

- RFC792: Internet Control Message Protocol
- RFC4443: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

1.2 Applications

Application	Description
End-to-End Connectivity Test	Both the network device and the destination host are connected to the IP network and configured with IP addresses.
Host Route Test	Both the network device and the destination host are connected to the IP network and configured with IP addresses.

1.2.1 End-to-End Connectivity Test

Scenario

As shown in Figure1-1, Network Device A and Target Host B are connected to the IP network.
If both the network device and the target host are connected to the IP network, the end-to-end connectivity test aims to check whether IP packets can be transmitted between the two ends. The target host can be the network device itself. In this case, the connectivity test aims to check the network interface and TCP/IP configurations on the device.

Figure1-1

Deployment

Execute the ping function on the network device.

1.2.2 Host Route Test

Scenario

As shown in Figure1-2, Network Device A and Target Host B are connected to the IP network.

If both the network device and the target host are connected to the IP network, the host route test aims to check gateways (or routers) that IP packets pass through between the two ends. Generally, the target host is not within the same IP network segment as the network device.

Figure1-2

Deployment

Execute the traceroute function on the network device.

1.3 Features

Overview

Feature	Description
Ping Test	Test whether the specified IPv4 address is reachable and display the related information.
Traceroute Test	Display the gateways that IPv4 packets pass through when transmitted from the source to the destination.

1.3.1 Ping Test

Working Principle

The ping tool sends an Internet Control Message Protocol (ICMP) Request message to the destination host to request the for an ICMP Echo Reply message. In this way, the ping tool determines the delay and the connectivity between the two network devices.

Related Configuration

- Run the **ping** command.

2 Traceroute Test

Working Principle

The traceroute tool uses the Time To Live (TTL) field in the headers of the ICMP and IP messages for the test First, the traceroute tool on the network device sends an ICMP Request message with TTL 1 to the destination host. After receiving the message, the first router on the path decreases the TTL by 1. As the TTL becomes 0, the router drops the packets and returns an ICMP time exceeded message to the network device. After receiving this message, the traceroute tool learns that this router exists on this path, and then sends an ICMP Request packet with TTL 2 to the destination host to discover the second router. Each time the traceroute tool increases the TTL in the ICMP Request message by 1 to discover one more router. This process is repeated until a data packet reaches the destination host. After the packet reaches the destination host, the host returns an ICMP Echo message instead of an ICMP time exceeded message to the network device. Then, the traceroute tool finishes the test and displays the path from the network device to the destination host.

Related Configuration

- Run the **traceroute** command.

2.1 Configuration

SG-5110 products support IPv6 ping and IPv6 traceroute tests.

Configuration	Description and Command	
Ping Test	(Optional) It is used to check whether an IPv4 address is reachable.	
	ping	Executes the Ping function.
Traceroute Test	(Optional) It is used to display the gateways that IPv4 packets pass through when transmitted from the source to the destination.	
	traceroute	Executes the traceroute function.

2.1.1 Ping Test

Configuration Effect

After conducting a ping test on a network device, you can learn whether the network device is connected to the destination host and whether packets can be transmitted between the network device and the destination host.

Notes

The network device must be configured with an IP address.

Configuration Steps

- To check whether an IPv4 address is reachable, use the **ping IPv4** command.
- To check whether an IPv6 address is reachable, use the **ping IPv6** command.

Verification

Run the ping command to display related information on the command line interface (CLI) window.

Related Commands

Ping IPv4

Command	**ping** [**oob** | **ip**] { *address* [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*] [**df-bit**] [**validate**] [**detail**] [**interval** millisecond] [**out-interface** interface [**next-hop** *next-hop*]] } **ping** [**ip**] { *address* [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*] [**df-bit**] [**validate**] [**detail**] [**interval** *millisecond*] [**out-interface** *interface* [**next-hop** *next-hop*]] }
Parameter Description	**oob**: Indicates out-of-band management. This parameter must be configured if the MGMT port is specified as the source port. *address*: Specifies the destination IPv4 address or domain name. *length*: Specifies the length of the data packet. The value ranges from 36 to 18,024. The default length is 100. *times*: Specifies the number of probes. The value ranges from 1 to 4,294,967,295 *seconds*: Specifies the timeout. The value ranges from 1s to 10s.

	data: Specifies the data in the packet. The data is a string of 1 to 255 bytes. By default, the string is "abcd". *source*: Specifies the source IPv4 address or source port of the packet. The loopback interface address, for example, 127.0.0.1, cannot be used as the source address. **df-bit**: Configures the DF bit of the IP address. When the DF bit is set to 1, the packet is not fragmented. By default, the DF bit is 0. **validate**: Configures whether to verify the response packet. **detail**: Configures whether to display the Echo Reply message in detail. By default, only the exclamation mark (!) and dot (.) are displayed. *interface*: Specifies the interface for sending the data packets. *next-hop*: Specifies the next hop IPv4 address. *millisecond*: Specifies the interval at which the ping packet is sent. The value ranges from 10 ms to 300,000 ms. The default interval is 100 ms.
Command Mode	In User EXEC mode, you can execute only the basic ping function. In Privileged EXEC mode, you can execute the extended ping function. In other configuration modes, you can run the **do** command to execute the extended ping function. For details about the configuration, see the description about the **do** command.
Configuration Usage	When the ping function is executed, information about the response (if any) will be displayed, and then related statistics will be output. Using the extended ping function, you can specify the number, length and timeout of packets to be sent. Like the basic ping function, related statistics will be output. To use the domain name, you must first configure the domain name server (DNS). For details about the configuration, see *Configuring DNS*.

Ping IPv6

Command	**ping** [**vrf** *vrf-name* | [**oob**] **ipv6**] [*address* [**via** *mgmt-name*] [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*] [**detail**] [**interval** millisecond] [**out-interface** interface [**next-hop** *next-hop*]]] **ping** [**oob** | **ipv6**] { *address* [**via** *mgmt-name*] [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*] [**df-bit**] [**validate**] [**detail**] [**interval** millisecond] [**out-interface** interface [**next-hop** *next-hop*]] } **ping** [**vrf** *vrf-name* | **ipv6**] { *address* [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*] [**df-bit**] [**validate**] [**detail**] [**interval** millisecond] [**out-interface** interface [**next-hop** *next-hop*]] } **ping** [**ipv6**] { *address* [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*] [**df-bit**] [**validate**] [**detail**] [**interval** millisecond] [**out-interface** interface [**next-hop** *next-hop*]] }
Parameter Description	**oob**: Indicates out-of-band management. This parameter must be configured if the MGMT port is specified as the source port. *vrf-name*: Indicates the VRF name. *address*: Specifies the destination IPv6 address or domain name. *mgmt-name:* Specifies the MGMT port in OOB mode.

	length: Specifies the length of data packet. The value ranges from 16 to 18,024. The default length is 100. *times*: Specifies the number of probes. The value ranges from 1 to 4,294,967,295. *seconds*: Specifies the timeout. The value ranges from 1s to 10s. *data*: Specifies the data in the packet. The data is a string of 1 to 255 bytes. *source*: Specifies the source IPv6 address or source port of the packet. The loopback interface address, for example, ::1, cannot be used as the source address. **detail**: Configures whether to display the Echo Reply message in detail. By default, only the exclamation mark (!) and dot (.) are displayed. *interface*: Specifies the interface for sending the data packets. *next-hop*: Specifies the next hop IPv6 address. *millisecond*: Specifies the interval at which the ping packet is sent. The value ranges from 10 ms to 300,000 ms. The default interval is 100 ms.
Command Mode	In User EXEC mode, you can execute only the basic ping IPv6 function. In Privileged EXEC mode, you can execute the extended ping IPv6 function. In other configuration modes, you can run the **do** command to execute the extended ping function. For details about the configuration, see the description about the **do** command.
Configuration Usage	When the ping IPv6 function is executed, information about the response (if any) will be displayed, and then related statistics will be output. Using the extended ping IPv6 function, you can specify the number, length and timeout of packets to be sent. Like the basic ping IPv6 function, related statistics will be output. To use the domain name, you must first configure the DNS. For details about the configuration, see *Configuring DNS*.

Configuration Example

Executing the Common Ping Function

Configuration Steps	In Privileged EXEC mode, run the **ping 192.168.21.26** command.
	Common ping command: FS# ping 192.168.21.26 Sending 5, 100-byte ICMP Echoes to 192.168.21.26, timeout is 2 seconds: < press Ctrl+C to break > !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms Detailed ping command: FS#ping 192.168.21.26 detail Sending 5, 100-byte ICMP Echoes to 192.168.21.26, timeout is 2 seconds: < press Ctrl+C to break > Reply from 192.168.21.26: bytes=100 time=4ms TTL=64

	Reply from 192.168.21.26: bytes=100 time=3ms TTL=64 Reply from 192.168.21.26: bytes=100 time=1ms TTL=64 Reply from 192.168.21.26: bytes=100 time=1ms TTL=64 Reply from 192.168.21.26: bytes=100 time=1ms TTL=64 Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms.
Verification	Send five 100-byte packets to the specified IP address, and the response information will be displayed in the specified time (2s by default). Finally the statistics is output.

Executing the Extended Ping Function

Configuration Steps	In Privileged EXEC mode, run the **ping 192.168.21.26** command. In addition, specify the length, number, and timeout of the packets.
	Common ping command: FS# ping 192.168.21.26 length 1500 ntimes 100 data ffff source 192.168.21.99 timeout 3 Sending 100, 1500-byte ICMP Echoes to 192.168.21.26, timeout is 3 seconds: < press Ctrl+C to break > !! Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms Detailed ping command: ping 192.168.21.26 length 1500 ntimes 20 data ffff source 192.168.21.99 timeout 3 detail Sending 20, 1500-byte ICMP Echoes to 192.168.21.26, timeout is 3 seconds: < press Ctrl+C to break > Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=2ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64

	Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=3ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Success rate is 100 percent (20/20), round-trip min/avg/max = 1/1/3 ms.
Verification	Send twenty 1500-byte packets to the specified IP address, and the response information (if any) will be displayed in the specified time (3s by default). Finally the statistics is output.

Executing the Common Ping IPv6 Function

Configuration Steps	In Privileged EXEC mode, run the **ping ipv6 2001::1** command.
	Common ping command: FS# ping ipv6 2001::1 Sending 5, 100-byte ICMP Echoes to 2001::1, timeout is 2 seconds: < press Ctrl+C to break > !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms Detailed ping command: FS#ping 2001::1 detail Sending 5, 100-byte ICMP Echoes to 2001::1, timeout is 2 seconds: < press Ctrl+C to break > Reply from 2001::1: bytes=100 time=1ms Reply from 2001::1: bytes=100 time=1ms Reply from 2001::1: bytes=100 time=1ms Reply from 2001::1: bytes=100 time=1ms Reply from 2001::1: bytes=100 time=1ms

	Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
Verification	Send five 100-byte packets to the specified IP address, and the response information will be displayed in the specified time (2s by default). Finally the statistics is output.

Executing the Extended Ping IPv6 Function

Configuration Steps	In Privileged EXEC mode, run the **ping ipv6 2001::5** command. In addition, specify the length, number, and timeout of the packets.
	Common ping command: FS# ping ipv6 2001::5 length 1500 ntimes 100 data ffff source 2001::9 timeout 3 Sending 100, 1500-byte ICMP Echoes to 2000::1, timeout is 3 seconds: < press Ctrl+C to break > !! Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms Detailed ping command: FS#ping 2001::5 length 1500 ntimes 10 data ffff source 2001::9 timeout 3 Sending 10, 1500-byte ICMP Echoes to 2001::5, timeout is 3 seconds: < press Ctrl+C to break > Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/1 ms.
Verification	Send one hundred 1500-byte packets to the specified IPv6 address, and the response information (if any) will be displayed in the specified time (3s by default). Finally the statistics is output.

2.1.2 Traceroute Test

Configuration Effect

After conducting a traceroute test on a network device, you can learn about the routing topology between the network device and the destination host, and the gateways through which packets are sent from the network device to the destination host.

Notes

The network device must be configured with an IP address.

Configuration Steps

- To trace the route an IPv4 packet would follow to the destination host, run the **traceroute IPv4** command.
- To trace the route an IPv6 packet would follow to the destination host, run the **traceroute IPv6** command.

Verification

Run the traceroute command to display related information on the CLI.

Related Commands

Traceroute IPv4

Command	**traceroute** [**oob** | **ip**] { *adress* [**probe** *number*] [**source** *source*] [**timeout** *seconds*] [**ttl** *minimum maximum*] [**out-interface** interface [**next-hop** *next-hop*]]] **traceroute**[**oob** | **ip**] { *adress* [**probe** *number*] [**source** *source*] [**timeout** *seconds*] [**ttl** *minimum maximum*] [**out-interface** *interface* [**next-hop** *next-hop*]] } **traceroute** [**ip**] { *adress* [**probe** *number*] [**source** *source*] [**timeout** *seconds*] [**ttl** *minimum maximum*] [**out-interface** *interface* [**next-hop** *next-hop*]]] **traceroute** [**ip**] { *adress* [**probe** *number*] [**source** *source*] [**timeout** *seconds*] [**ttl** *minimum maximum*] [**out-interface** *interface* [**next-hop** *next-hop*]] }
Parameter Description	**oob**: Indicates out-of-band management. This parameter must be configured if the MGMT port is specified as the source port. *address*: Specifies the destination IPv4 address or domain name. *mgmt-name:* Specifies the MGMT port in OOB mode. *number*: Specifies the number of probes. The value ranges from 1 to 255. *source*: Specifies the source IPv4 address or source port of the packet. The loopback interface address, for example, 127.0.0.1, cannot be used as the source address. *seconds*: Specifies the timeout. The value ranges from 1s to 10s. *minimum maximum*: Specifies the minimum and maximum TTL values. The value ranges from 1 to 255. *interface*: Specifies the interface for sending the data packets. *next-hop*: Specifies the next hop IPv4 address.

Command Mode	In User EXEC mode, you can execute only the basic traceroute function. In privileged EXEC mode, you can execute the extended traceroute function.
Configuration Usage	The **traceroute** command is used to test the network connectivity and accurately locate a fault when the fault occurs. To use the domain name, you must first configure the DNS. For details about the configuration, see *Configuring DNS*.

Traceroute IPv6

Command	**traceroute** [[**oob**] **ipv6**] { *address* [**via** *mgmt-name*] [**probe** *number*] [**timeout** *seconds*] [**ttl** *minimum maximum*] [**out-interface** interface [**next-hop** *next-hop*]] } **traceroute** [[**oob**] **ipv6**] { *address* [**via** *mgmt-name*] [**probe** *number*] [**timeout** *seconds*] [**ttl** *minimum maximum*] [**out-interface** interface [**next-hop** *next-hop*]] } **traceroute** [**ipv6**] { *address* [**probe** *number*] [**timeout** *seconds*] [**ttl** *minimum maximum*] [**out-interface** interface [**next-hop** *next-hop*]] } **traceroute** [**ipv6**] { *address* [**probe** *number*] [**timeout** *seconds*] [**ttl** *minimum maximum*] [**out-interface** interface [**next-hop** *next-hop*]] }
Parameter Description	**oob**: Indicates out-of-band management. This parameter must be configured if the MGMT port is specified as a source port. *vrf-name*: Indicates the VRF name. *address*: Specifies the destination IPv6 address or domain name. *mgmt-name:* Specifies the MGMT port in OOB mode. *number*: Specifies the number of probes. The value ranges from 1 to 255. *seconds*: Specifies the timeout. The value ranges from 1s to 10s. *minimum maximum*: Specifies the minimum and maximum TTL values. The value ranges from 1 to 255. *interface*: Specifies the interface for sending the data packets. *next-hop*: Specifies the next hop IPv6 address.
Command Mode	In User EXEC mode, you can execute only the basic traceroute IPv6 function. In privileged EXEC mode, you can execute the extended traceroute IPv6 function.
Configuration Usage	The traceroute IPv6 command is used to test the network connectivity and accurately locate a fault when the fault occurs. To use the domain name, you must first configure the DNS. For details about the configuration, see *Configuring DNS*.

Configuration Example

Executing the Traceroute Function on a Properly Connected Network

Configuration Steps	In Privileged EXEC mode, run the **traceroute ipv6 3004::1** command.

```
FS#
FS# traceroute ipv6 3004::1
  < press Ctrl+C to break >
Tracing the route to 3004::1
1        3000::1          0 msec   0 msec   0 msec
2        3001::1          4 msec   4 msec 4 msec
3        3002::1          8 msec   8 msec   4 msec
```

The preceding test result indicates that the network device accesses host 3004::1 by transmitting packets through gateways 1–3. In addition, the time required to reach each gateway is displayed.

Executing the Traceroute Function on a Faulty Network

Configuration Steps	In Privileged EXEC mode, run the **traceroute 202.108.37.42** command.

```
FS# traceroute 202.108.37.42
< press Ctrl+C to break >
Tracing the route to 202.108.37.42
1        192.168.12.1        0 msec   0 msec   0 msec
2        192.168.9.2         0 msec   4 msec 4 msec
3        192.168.110.1      16 msec   12 msec   16 msec
4        *   *   *
5        61.154.8.129        12 msec   28 msec   12 msec
6        61.154.8.17          8 msec   12 msec   16 msec
7        61.154.8.250        12 msec   12 msec   12 msec
8        218.85.157.222      12 msec   12 msec   12 msec
9        218.85.157.130      16 msec   16 msec   16 msec
10       218.85.157.77       16 msec   48 msec   16 msec
11       202.97.40.65        76 msec   24 msec   24 msec
12       202.97.37.65        32 msec   24 msec   24 msec
13       202.97.38.162       52 msec   52 msec   224 msec
14       202.96.12.38        84 msec   52 msec   52 msec
15       202.106.192.226     88 msec   52 msec   52 msec
16       202.106.192.174     52 msec   52 msec   88 msec
17       210.74.176.158     100 msec   52 msec   84 msec
18       202.108.37.42       48 msec   48 msec   52 msec
```

	The preceding test result indicates that the network device accesses host 202.108.37.42 by transmitting packets through gateways 1–17, and Gateway 4 is faulty.

Executing the Traceroute IPv6 Function on a Properly Connected Network

Configuration Steps	In Privileged EXEC mode, run the **traceroute ipv6 3004::1** command.
	FS# traceroute ipv6 3004::1 < press Ctrl+C to break > Tracing the route to 3004::1 1 3000::1 0 msec 0 msec 0 msec 2 3001::1 4 msec 4 msec 4 msec 3 3002::1 8 msec 8 msec 4 msec 4 3004::1 4 msec 28 msec 12 msec
	The preceding test result indicates that the network device accesses host 3004::1 by transmitting packets through gateways 1-4. In addition, the time required to reach each gateway is displayed.

Executing the Traceroute IPv6 Function on a Faulty Network

Configuration Steps	In Privileged EXEC mode, run the **traceroute ipv6 3004::1** command.
	FS# traceroute ipv6 3004::1 < press Ctrl+C to break > Tracing the route to 3004::1 1 3000::1 0 msec 0 msec 0 msec 2 3001::1 4 msec 4 msec 4 msec 3 3002::1 8 msec 8 msec 4 msec 4 * * * 5 3004::1 4 msec 28 msec 12 msec
	The preceding test result indicates that the network device accesses host 3004::1 by transmitting packets through gateways 1–5, and Gateway 4 is faulty.

3 Configuring DHCP

3.1 Overview

The Dynamic Host Configuration Protocol (DHCP) is a LAN protocol based on the User Datagram Protocol (UDP) for dynamically assigning reusable network resources, for example, IP addresses.

The DHCP works in Client/Server mode. A DHCP client sends a request message to a DHCP server to obtain an IP address and other configurations. When a DHCP client and a DHCP server are not in a same subnet, they need a DHCP relay to forward DHCP request and reply packets.

Protocols and Standards

- RFC2131: Dynamic Host Configuration Protocol
- RFC2132: DHCP Options and BOOTP Vendor Extensions
- RFC3046: DHCP Relay Agent Information Option

3.2 Applications

Application	Description
Providing DHCP Service in a LAN	Assigns IP addresses to clients in a LAN.
Enabling DHCP Client	Enable DHCP Client.
Deploying DHCP Relay in Wired Network	In a wired network, users from different network segments requests IP addresses.

3.2.1 Providing DHCP Service in a LAN

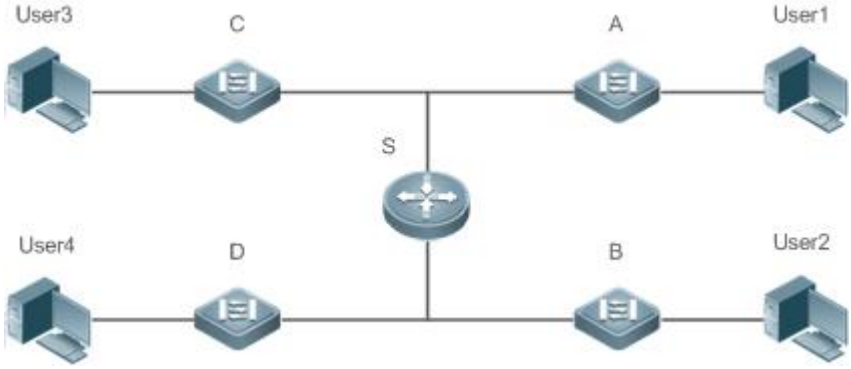
Scenario

Assign IP addresses to four users in a LAN.

For example, assign IP addresses to User 1, User 2, User 3 and User 4, as shown in the following figure.

- The four users are connected to Server S through A, B, C and D.

Figure 2-1



Remarks	S is an egress gateway working as a DHCP server.

	A, B, C and D are access switches achieving layer-2 transparent transmission. User 1, User 2, User 3 and User 4 are LAN users.

Deployment

- Enable DHCP Server on S.
- Deploy layer-2 VLAN transparent transmission on A, B, C and D.
- User 1, User 2, User 3 and User 4 initiate DHCP client requests.

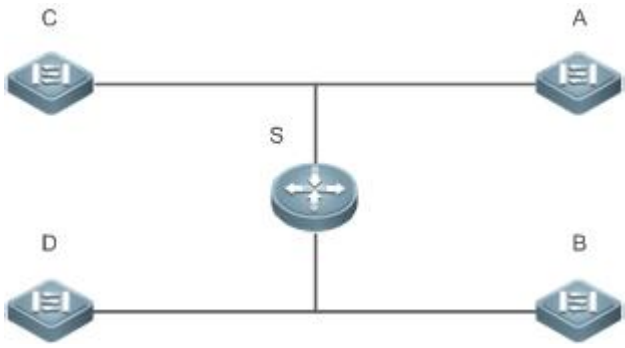
3.2.2 Enabling DHCP Client

Scenario

Access switches A, B, C and D in a LAN request server S to assign IP addresses.

For example, enable DHCP Client on the interfaces of A, B, C and D to request IP addresses, as shown in the following figure.

Figure 2-2



Remarks	S is an egress gateway working as a DHCP server. A, B, C and D are access switches with DHCP Client enabled on the interfaces.

Deployment

- Enable DHCP Server on S.
- Enable DHCP Client on the interfaces of A, B, C and D.

3.2.3 Deploying DHCP Relay in Wired Network

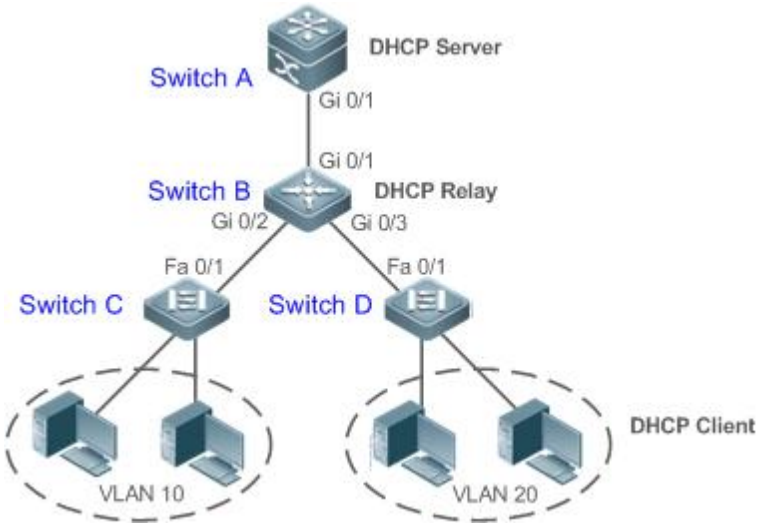
Scenario

As shown in the following figure, Switch C and Switch D are access devices for the users in VLAN 10 and VLAN 20 respectively. Switch B is a gateway, and Switch A is a core device. The requirements are listed as follows:

Switch A works as a DHCP server to assign IP addresses of different network segments dynamically to users in different VLANs.

Users in VLAN 10 and VLAN 20 obtain IP addresses dynamically.

Figure 2-3 DHCP Relay



Remarks	Switch C and Switch D are access devices. Switch B is a gateway. Switch A is a core device.

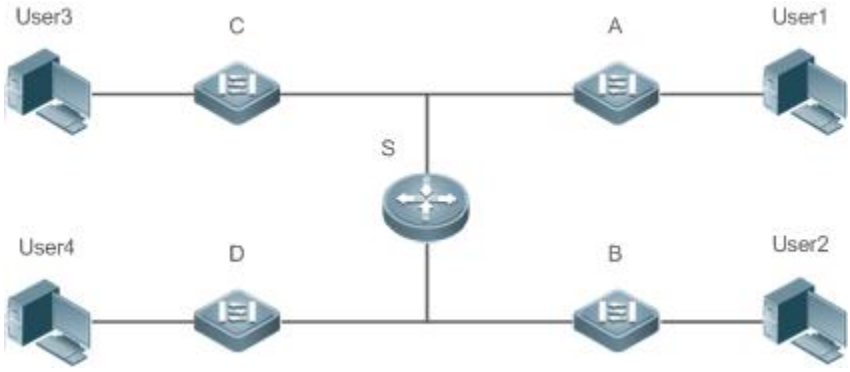
Deployment

- Configure layer-2 communication between Switch B and Switch C as well as between Switch B and Switch D.
- On Switch B, specify a DHCP server address and enable DHCP Relay.
- On Switch A, create DHCP address pools for VLAN 10 and VLAN 20 respectively, and enable DHCP Server.

3.2.4 Assigning Static IP Addresses

Scenario

An administrator wants to assign static IP addresses to internal and external servers to facilitate policy management. In medical scenarios, a department may have the desire of having devices assigned static IP addresses, which will not be changed even after device replacement. In small- and medium-sized enterprises, there is also a demand for assigning static IP addresses based on employee IDs to identify users.



Remarks	S is an egress gateway and works as the DHCP server. A, B, C and D are access switches achieving layer-2 transparent transmission. User1, User2, User3 and User4 are users.

Deployment

- Run the DHCP server on S.
- Enable DHCP snooping on A, B, C and D.
- Obtain the MAC addresses and host names of User1, User2, User3 and User4.
- Obtain the addresses, ports, and VLANs of access devices at the access locations of User1, User2, User3 and User4.
- On server S, bind a static IP address to a specified MAC address, access location, and host name.
- User1, User2, User3 and User4 initiate DHCP client requests.

3.3 Features

Basic Concepts

DHCP Server

Based on the RFC 2131, FS DHCP server assigns IP addresses to clients and manages these IP addresses.

DHCP Client

DHCP Client enables a device to automatically obtain an IP address and configurations from a DHCP server.

DHCP Relay

When a DHCP client and a DHCP server are not in a same subnet, they need a DHCP relay to forward DHCP request and reply packets.

Lease

Lease is a period of time specified by a DHCP server for a client to use an assigned IP address. An IP address is active when leased to a client. Before a lease expires, a client needs to renew the lease through a server. When a lease expires or is deleted from a server, the lease becomes inactive.

Excluded Address

An excluded address is a specified IP address not assigned to a client by a DHCP server.

Address Pool

An address pool is a collection of IP addresses that a DHCP server may assign to clients.

Option Type

An option type is a parameter specified by a DHCP server when it provides lease service to a DHCP client. For example, a public option include the IP addresses of a default gateway (router), WINS server and a DNS server. DHCP server allows configuration of other options. Though most options are defined in the RFC 2132, you can add user-defined options.

Overview

Feature	Description
DHCP Server	Enable DHCP Server on a device, and it may assign IP addresses dynamically and pushes configurations to DHCP clients.

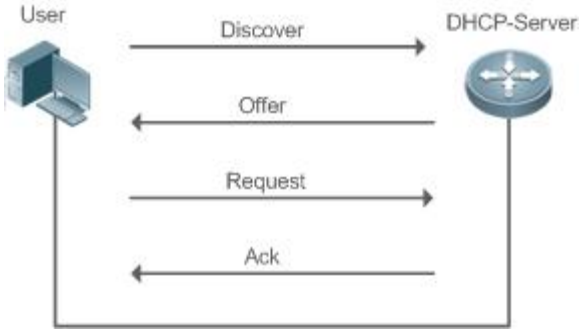
Feature	Description
DHCP Relay Agent	Enable DHCP Relay on a device, and it may forward DHCP request and reply packets across different network segments.
DHCP Client	Enable DHCP Client on a device, and it may obtain IP addresses and configurations automatically from a DHCP server.

3.3.1 DHCP Server

Working Principle

DHCP Working Principle

Figure 2-4



A host requests an IP address through DHCP as follows:

1. A host broadcasts a DHCP discover packet to find DHCP servers in a network.
2. DHCP servers unicast/broadcast (based on the property of the host packet) DHCP offer packets to the host, containing an IP address, a MAC address, a domain name and a lease.
3. The host broadcasts a DHCP request packet to formally request an IP address.
4. A DHCP server sends a DHCP ACK unicast packet to the host to acknowledge the request.

A DHCP client may receive DHCPOFFER packets from multiple DHCP servers, but usually it accepts only the first DHCPOFFER packet. Besides, the address specified in a DHCPOFFER packet is not necessarily assigned. Instead, it is retained by the DHCP server until a client sends a formal request.

To formally request an IP address, a client broadcasts a DHCPREQUEST packet so that all DHCP servers sending DHCPOFFER packets may receive the packet and release OFFER IP addresses.

If a DHCPOFFER packet contains invalid configuration parameters, a client will send a DHCPDECLINE packet to the server to decline the configuration.

During the negotiation, if a client does not respond to the DHCPOFFER packets in time, servers will send DHCPNAK packets to the client and the client will reinitiate the process.

During network construction, FS DHCP servers have the following features:

- Low cost. Usually the static IP address configuration costs more than DHCP configuration.
- Simplified configuration. Dynamic IP address assignment dramatically simplifies device configuration
- Centralized management. You can modify the configuration for multiple subnets by simply modifying the DHCP server configuration.

Address Pool

After a server receives a client's request packet, it chooses a valid address pool, determines an available IP address from the pool through PING, and pushes the pool and address configuration to the client. The lease information is saved locally for validity check upon lease renewal.

An address pool may carry various configuration parameters as follows:

- An IP address range, which is the range of IP addresses that are available.
- A gateway address. A maximum of 8 gateway addresses are supported.
- A DNS address. A maximum of 8 DNS addresses are supported.
- A lease period notifying clients of when to age an address and request a lease renewal.

VRRP Monitoring

In a Virtual Router Redundancy Protocol (VRRP) scenario, FS devices enabled with DHCP provide a command to monitor the VRRP status of the interface. To an interface configured with VRRP address and VRRP monitoring, a DHCP server only processes the DHCP clients' request packets from the interface in Master state, and other packets are discarded. If no VRRP address is configured, the DHCP server does not monitor the VRRP status, and all DHCP packets are processed. VRRP monitoring is configured on only layer-3 interfaces. It is disabled by default, namely, only the Master device processes the DHCP service.

Adding Trusted ARP

A trusted ARP prevents gateway ARP spoofing. FS devices enabled with DHCP provide a command for pushing a trusted ARP while assigning an address. After this function is enabled, DHCP server pushes it while assigning an IP address to the client to prevent ARP spoofing.

Adding Pseudo Server Detection

If a DHCP server is deployed illegally, a client interacts with this server while requesting an IP address and a wrong address will be assigned to the client. This server is a pseudo server. FS devices enabled with DHCP provides a command to enable pseudo server detection. After it is enabled, DHCP packets are checked for Option 54 (Server Identifier Option). If the content of Option 54 is different from the actual DHCP server identifier, the IP address of the pseudo server and port receiving the packets will be recorded. The pseudo server detection is only an after-event security function and cannot prevent an illegal DHCP server from assigning IP addresses to clients.

Related Configuration

Enabling DHCP Server Globally

- By default, DHCP Server is disabled.
- Run the **service dhcp** command to enable the DHCP Server.
- Run the **service dhcp** command globally to enable DHCP service.

Configuring Address Pool

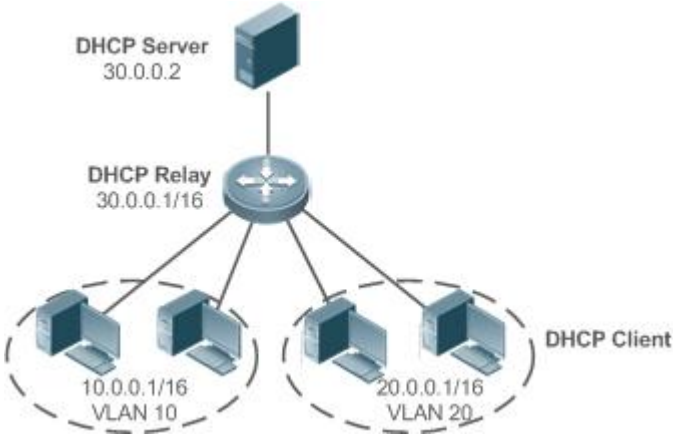
- By default, no address pool is configured.
- Run the **ip dhcp pool** command to configure an IP address range, a gateway and a DNS.
- If no address pool is configured, no addresses will be assigned.

3.3.2 DHCP Relay Agent

Working Principle

The destination IP address of DHCP request packets is 255.255.255.255, and these packets are forwarded within a subnet. To achieve IP address assignment across network segments, a DHCP relay agent is needed. The DHCP relay agent unicasts DHCP request packets to a DHCP server and forwards DHCP reply packets to a DCHP client. The DHCP relay agent serves as a repeater connecting a DHCP client and a DHCP server of different network segments by forwarding DHCP request packets and DHCP reply packets. The Client-Relay-Server mode achieves management of IP addresses across multiple network segments by only one DHCP server. See the following figure.

Figure 2-5 DHCP Relay Scenario



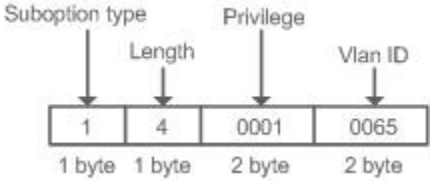
VLAN 10 and VLAN 20 correspond to the segments 10.0.0.1/16 and 20.0.0.1/16 respectively. A DHCP server with IP address 30.0.0.2 is in segment 30.0.0.1/16. To achieve management of dynamic IP addresses in VLAN 10 and VLAN 20 by the DHCP server, you only need to enable DHCP Relay on a gateway and configure IP address 30.0.0.2 for the DHCP server.

➘ DHCP Relay Agent Information (Option 82)

As defined in RFC3046, an option can be added to indicate a DHCP client's network information when DHCP Relay is performed, so that a DHCP server may assign IP addresses of various privileges based on more accurate information. The option is called Option 82. Currently, FS devices support four schemes of relay agent information, which are described respectively as follows:

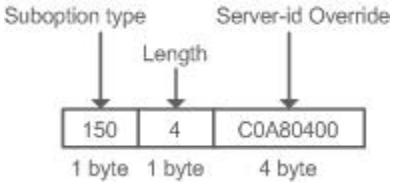
1. Relay agent information option dot1x: This scheme should be implemented with 802.1X authentication and the FS-SAM products. Specifically, FS-SAM products push the IP privilege during 802.1X authentication. A DHCP relay agent forms a Circuit ID sub-option based on the IP privilege and the VLAN ID of a DHCP client. The option format is shown in the following figure.

Figure 2-6 Option Format



2. Relay agent information option82: This scheme serves without correlation with other protocol modules. A DHCP relay agent forms an Option 82 based on the physical port receiving DHCP request packets and the MAC address of the device. The option format is shown in the following figure.

Figure 2-7 Server-Identifier-Override



3. Relay agent information option82: This scheme serves without correlation with other protocol modules. Compared with previous Option 82, this option supports user-defined content, which may change. By default, a DHCP relay agent forms Option 82 according to the information of the physical port receiving DHCP packets, device MAC address and device name. The option format is shown in the following figure.

Figure 2-8 Option82.1-circuit-id

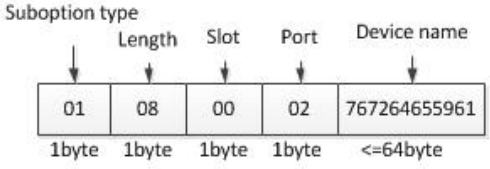
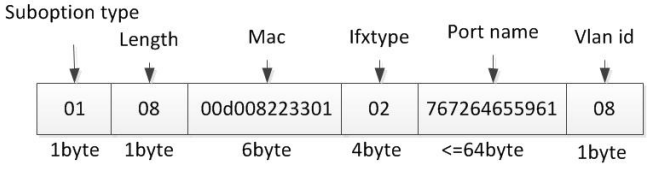


Figure 2-9 Option82-remote-id



DHCP Relay Check Server-ID

In DHCP environment, multiple DHCP servers are deployed for a network, achieving server backup to ensure uninterrupted network operation. After this function is enabled, the DHCP request packet sent by a client contains a **server-id** option specifying a DHCP server. In alleviating the burden on servers in specific environments, you need to enable this function on a relay agent to send a packet to a specified DHCP server rather than all DHCP servers.

DHCP Relay suppression

After you configure the ip dhcp relay suppression command on an interface, DHCP request packets received on the interface will be filtered, and the other DHCP request packets will be forwarded.

Related Configuration

Enabling DHCP Relay

- By default, DHCP Relay is disabled.
- You may run the **service dhcp** command to enable DHCP Relay.
- You need to enable DHCP Relay before it works.

Configuring IP Address for DHCP Server

- By default, no IP address is configured for a DHCP server.

- You may run the **ip helper-address** command to configure an IP address for a DHCP server. The IP address can be configured globally or on a layer-3 interface. A maximum of 20 IP addresses can be configured for a DHCP server.
- When an interface receives a DHCP request packet, the DHCP server configuration on the interface prevails over that configured globally. If the interface is not configured with DHCP server addresses, the global configuration takes effect.

Enabling DHCP Option 82

- By default, DHCP Option 82 is disabled.
- You may run the **ip dhcp relay information option82** command to enable DHCP Option 82.

Enabling DHCP Relay Check Server-ID

- By default, DHCP Relay check server-id is disabled.
- You may run the **ip dhcp relay check server-id** command to enable DHCP Relay check server-id.

Enabling DHCP Relay Suppression

- By default, DHCP Relay suppression is disabled on all interfaces.
- You may run the **ip dhcp relay suppression** command to enable it on an interface.

3.3.3 DHCP Client

Working Principle

A DHCP client broadcasts a DHCP discover packet after entering the Init state. Then it may receive multiple DHCP offer packets. It chooses one of them and responds to the corresponding DHCP server. After that, it sends lease renewal request packets in the Renew and Rebind processes of an aging period to request lease renewal.

Related Configuration

Enabling DHCP Client on Interface

- By default, DHCP Client is disabled.
- In interface configuration mode, you may run the **ip address dhcp** command to enable DHCP Client.
- You need to enable DHCP Client to enable DHCP service.
- The configuration takes effect on a layer-3 interface, for example, an SVI or a routed port.

3.3.4 Assignment of Static IP Addresses

Working Principle

In a DHCP request packet, the option carries the host name, terminal address, and access location. The administrator binds a static IP address to a specified host name, access location, and terminal MAC address. When the terminal requests to go online, and the static IP address is assigned to the terminal after the packet of the terminal matches the binding information.

Related Configuration

Run the following command to bind and assign a static IP address to a specified access location, host name, and terminal MAC address:

ip dhcp add-client { **solidify-ip ip** *ip-addr* { { **access-device** *dev-addr* **access-vlan** *vlanid* **access-port** *portid* | **host-name** *hostname* | **mac** *mac-addr* } **binding-type** { **ip-hostname** | **ip-hostname-location** | **ip-mac** | **ip-mac-hostname** | **ip-mac-hostname-location** | **ip-mac-location** } } | **solidify-location ip** *ip-addr* **access-device** *dev-addr* **access-vlan** *vlanid* **access-port** *portid* | **solidify-mac mac** *mac-addr*}

3.4 Configuration

Configuring DHCP Server

Configuration	Description and Command	
Configuring Dynamic IP Address	(Mandatory) It is used to enable DHCP Server to achieve dynamic IP address assignment.	
	service dhcp	Enables DHCP Server.
	ip dhcp pool	Configures an address pool.
	network	Configures the network number and subnet mask of a DHCP address pool.
	(Optional) It is used to configure the properties of an address pool.	
	default-router	Configures a default gateway of a client.
	lease	Configures an address lease.
	next-server	Configures a TFTP server address
	bootfile	Configures a boot file of a client.
	domain-name	Configures a domain name of a client.
	dns-server	Configures a domain name server.
	netbios-name-server	Configures a NetBIOS WINS server.
	netbios-node-type	Configures a NetBIOS node type on a client.
	lease-threshold	Configures an alarm threshold of an address pool.
	option	Configures a user-defined option.
	pool-status	Enables or disables an address pool.
	update arp	Adds a trusted ARP while assigning addresses from a pool.

Configuring DHCP Relay

Configuration	Description and Command	
Configuring Basic DHCP Relay Functions	(Mandatory) It is used to enable DHCP Relay.	
	service dhcp	Enables DHCP Relay.
	ip helper-address	Configures an IP Address of a DHCP Server.

Configuration	Description and Command	
Configuring DHCP Relay Option 82	(Optional) It is used to assign IP addresses of different privileges to clients in combination with the information of a physical port. This function cannot be used together with the **dhcp option dot1x** command.	
	ip dhcp relay information option82	Enables DHCP option82.
Configuring DHCP Relay Check Server-ID	(Optional) It is used to enable a DHCP Relay agent to send DHCP request packets only to a specified server.	
	ip dhcp relay check server-id	Enables a DHCP Relay agent to send DHCP request packets only to a specified server
Configuring DHCP Relay Suppression	(Optional) It is used to shield DHCP request packets on an interface.	
	ip dhcp relay suppression	Enables DHCP Relay Suppression.

Configuring DHCP Client

Configuration	Description and Command	
Configuring DHCP Client	(Mandatory) It is used to enable DHCP Client.	
	ip address dhcp	Enables an Ethernet interface, a PPP/HDLC-encapsulated or FR-encapsulated interface to obtain IP addresses through DHCP.

Assigning Static IP Addresses

Configuration	Description and Command	
Assigning Static IP Addresses	(Optional) It is used to bind and assign a static IP address to an access location, host name, and terminal MAC address. In addition, it can be used to bind a single MAC address of a terminal in authorized address assignment mode.	
	ip dhcp add-client { solidify-ip ip *ip-addr* **{ { access-device** *dev-addr* **access-vlan** *vlanid* **access-port** *portid* **| host-name** *hostname* **| mac** *mac-addr* **} binding-type { ip-hostname | ip-hostname-location | ip-mac | ip-mac-hostname | ip-mac-hostname-location | ip-mac-location } } | solidify-location ip** *ip-addr* **access-device** *dev-addr* **access-vlan** *vlanid* **access-port** *portid* **| solidify-mac mac** *mac-addr*}	Binds and assigns a static IP address to any combination of a specified access location, host name, and terminal MAC address. In authorized address assignment mode, assigns an IP address to a terminal whose information is bound.

3.4.1 Configuring Dynamic IP Address

Configuration Effect

Provide all DHCP clients with DHCP service including assigning IP addresses and gateways.

Notes

A DHCP server and a DHCP relay share the service dhcp command, but a device cannot function as a DHCP server and relay at the same time. When a device is configured with a valid address pool, it acts as a server and forwards packets. Otherwise, it serves as a relay agent.

Configuration Steps

Enabling DHCP Server

- Mandatory. It achieves dynamic IP address assignment.
- Run the **service dhcp** command in global configuration mode.

Configuring Address Pool

- Mandatory. It is used to create an IP address pool.
- Run the **ip dhcp pool** command in global configuration mode.

Configuring Network Number and Subnet Mask of DHCP Address Pool

- Mandatory. It defines a range of dynamically assigned addresses.
- Run the **network** command in DHCP address pool configuration mode.

Configuring Default Gateway of Client

- Optional. It is used to configure a gateway address.
- Run the **default-router** command in DHCP address pool configuration mode.

Configuring Address Lease

- Optional. It is used to configure an IP address lease, which is 24h by default.
- Run the **lease** command in DHCP address pool configuration mode.

Configuring TFTP Server Address

- Optional. It is used to configure a TFTP server address.
- Run the **next-server** command in DHCP address pool configuration mode.

Configuring Domain Name of Client

- Optional. It is used to configure the domain name of a client.
- Run the **domain-name** command in DHCP address pool configuration mode.

Configuring DNS

- Optional. It is used to configure a DNS address.
- Run the **dns** command in DHCP address pool configuration mode.

Configuring NetBIOS WINS Server

- Optional. It is used to configure a NetBIOS WINS server address.

- Run the **netbios-name-server** command in DHCP address pool configuration mode.

Configuring NetBIOS Node Type on Client

- Optional. It is used to configure a NetBIOS node type.
- Run the **netbios-name-type** command in DHCP address pool configuration mode.

Configuring Alarm Threshold of Address Pool

- Optional. It is used to manage the number of leases. When a threshold (90% by default) is reached, an alarm will be printed.
- Run the **lease-threshold** command in DHCP address pool configuration mode.

Configuring User-Defined Option

- Optional. It is used to configure user-defined options.
- Run the **option** command in DHCP address pool configuration mode.

Enabling or Disabling Address Pool

- Optional. It is used to enable or disable an address pool. It is enabled by default.
- Run the **pool-status** command in DHCP address pool configuration mode.

Adding Trusted ARP

- Optional. It is used to add a trusted ARP while assigning an IP address. It is disabled by default.
- Run the **update arp** command in DHCP address pool configuration mode.

Configuring the Authorized Address Assignment Function for the Address Pool

- When a user request matches an IP address segment in the address pool, in which the authorized address assignment mode is enabled, an IP address can be assigned to the terminal only after the static IP address is bound to the terminal.
- Run the **solidify** command in DHCP address pool configuration mode.

Verification

Connect a DHCP client and a DHCP server.

- Check whether the client obtains configurations on the server.

Related Commands

Enabling DHCP Server

Command	**service dhcp**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Enable DHCP Server and DHCP Relay. A DHCP server and a DHCP relay share the **service dhcp** command. When a device is configured with a valid address pool, it acts as a server and forwards packets. Otherwise, it serves as a relay agent.

Configuring Address Pool

Command	**ip dhcp pool** *dhcp-pool*
Parameter Description	*pool-name*: Indicates the name of an address pool.
Command Mode	Global configuration mode
Usage Guide	Before assigning an IP address to a client, you need to configure an address pool name and enter DHCP address pool configuration mode.

Configuring Network Number and Subnet Mask of DHCP Address Pool

Command	**network** *network-number mask* [*low-ip-address high-ip-address*]
Parameter Description	*network-number:* Indicates the network number of an IP address pool. *mask:* Indicates the subnet mask of an IP address pool. If no subnet mask is defined, the natural subnet mask is applied.
Command Mode	DHCP address pool configuration mode
Usage Guide	To configure dynamic address assignment, you need to configure a network number and subnet mask of an address pool to provide a DHCP server with a range of addresses. The IP addresses in a pool are assigned in order. If an address is assigned or exists in the target network segment, the next address will be checked until a valid address is assigned. FS wireless products provide available network segments by specifying start and end addresses. The configuration is optional. If the start and end address are not specified, all IP addresses in the network segment are assignable. For FS products, addresses are assigned based on the client's physical address and ID. Therefore, one client will not be assigned two leases from one address pool. In case of topological redundancy between a client and a server, address assignment may fail. To avoid such failures, a network administrator needs to prevent path redundancy in network construction, for example, by adjusting physical links or network paths.

Configuring Default Gateway of Client

Command	**default-router** *address* [*address2…address8*]
Parameter Description	*address*: Indicates the IP address of a default gateway. Configure at least one IP address. *ip-address2…ip-address8:* (Optional) A maximum of 8 gateways can be configured.
Command Mode	DHCP address pool configuration mode
Usage Guide	Configure a default gateway of a client, and a server will push the gateway configuration to the client. The IP addresses of the default gateway and the client should be in a same network.

Configuring Address Lease

Command	**lease** {*days* [*hours]* [*minutes*] | **infinite**}
Parameter Description	*days:* Defines a lease in the unit of day. *hours:* (Optional) Defines a lease in the unit of hour. Please define *days* before *hours*. *minutes:* (Optional) Defines a lease in the unit of minute. Please define *days* and *hours* before *minutes*.

	infinite: Defines an unlimited lease.
Command Mode	DHCP address pool configuration mode
Usage Guide	The default lease of an IP address assigned by a DHCP server is 1 day. When a lease is expiring soon, a client needs to request a lease renewal. Otherwise the IP address cannot be used after the lease is expired.

Configures Boot File on Client

Command	**bootfile** *filename*
Parameter Description	*file-name*: Defines a boot file name.
Command Mode	DHCP address pool configuration mode
Usage Guide	A boot file is a bootable image file used when a client starts up. The file is usually an OS downloaded by a DHCP client.

Configuring Domain Name of Client

Command	**domain-name** *domain*
Parameter Description	*domain-name:* Defines a domain name of a DHCP client.
Command Mode	DHCP address pool configuration mode
Usage Guide	You may define a domain name for a client. When the client accesses network through the host name, the domain name will be added automatically to complete the host name.

Configuring DNS

Command	**dns-server** { *ip-address* [*ip-address2…ip-address8*] | **use-dhcp-client** *interface-type interface-number* }
Parameter Description	*ip-address:* Defines an IP address of a DNS server. Configure at least one IP address. *ip-address2…ip-address8:* (Optional) A maximum of 8 DNS servers can be configured. **use-dhcp-client** *interface-type interface-number:* A DHCP client learns its DNS server via FSOS software.
Command Mode	DHCP address pool configuration mode
Usage Guide	If a client accesses network resources through the domain name, you need to configure a DNS server to resolve the domain name.

Configuring NetBIOS WINS Server

Command	**netbios-name-server** *address* [*address2…address8*]
Parameter Description	*address:* Defines an IP address of a WINS server. Configure at least one IP address. *ip-address2…ip-address8:* (Optional) A maximum of 8 WINS servers can be configured.
Command Mode	DHCP address pool configuration mode
Usage Guide	WINS is a domain name service through which a Microsoft TCP/IP network resolves a NetNBIOS name to an IP address. A WINS server is a Windows NT server. When a WINS server starts, it receives a registration request from a WINS client. When the client shuts down, it sends a name release message, so that the computers in the WINS database and on the

	network are consistent.

Configuring NetBIOS Node Type on Client

Command	**netbios-node-type** *type*
Parameter Description	type: Defines a NetBIOS node type with one of the following approaches. 1. A hexadecimal number, ranging from 0 to FF. Only followings values are available. ● b-node ● p-node ● m-node ● 8 for h-node 2. A character string. ● b-node for a broadcast node; ● p-node for a peer-to-peer node; ● m-node for a mixed node; ● h-node for a hybrid mode.
Command Mode	DHCP address pool configuration mode
Usage Guide	There are four types of NetBIOS nodes of a Microsoft DHCP client. 1) A broadcast node. For such a node, NetBIOS name resolution is requested through broadcast.2) A peer-to-peer node. The client sends a resolution request to the WINS server. 3) A mixed node. The client broadcasts a resolution request and sends the resolution request to the WINS server.. 4) A hybrid node. The client sends a resolution request to the WINS server. If no reply is received, the client will broadcast the resolution request. By default, a Microsoft operating system is a broadcast or hybrid node. If no WINS server is configured, it is a broadcast node. Otherwise, it is a hybrid node.

Configuring User-Defined Option

Command	**option** *code* { **ascii** *string* | **hex** *string* | **ip** *ip-address* }
Parameter Description	*code:* Defines a DHCP option code. **ascii** *string:* Defines an ASCII character string. **hex** *string:* Defines a hexadecimal character string. **ip** *ip-address:* Defines an IP address.
Command Mode	DHCP address pool configuration mode
Usage Guide	The DHCP allows transmitting configuration information to a host via a TCP/IP network. DHCP packets contain the option field of definable content. A DHCP client should be able to receive a DHCP packet carrying at least 312 bytes option. Besides, the fixed data field in a DHCP packet is also called an option. In a WLAN, a DHCP client on an AP dynamically requests the IP address of an AC. You may configure on a DHCP server the **option** command specifying the AC address.

Enabling or Disabling Address Pool

Command	**pool-status** {**enable** | **disable**}

Parameter Description	**enable**: Enables an address pool. **disable**: Disable an address pool. It is enabled by default.
Command Mode	DHCP address pool configuration mode
Usage Guide	A FS wireless product provides a command for you to enable/disable a DHCP address pool.

Adding Trusted ARP

Command	**update arp**
Parameter Description	N/A
Command Mode	DHCP address pool configuration mode
Usage Guide	After configuration, a trusted ARP is added when an address is assigned from a pool. A trusted ARP prevents ARP spoofing.

Configuring the Authorized Address Assignment Mode

Command	**solidify**
Parameter Description	N/A
Command Mode	DHCP address pool configuration mode
Usage Guide	After this function is enabled for a DHCP server address pool, when a terminal hits the address pool, an IP address can be assigned to the terminal only in the case that a static IP address has been bound to the terminal.

Configuration Example

Configuring Address Pool

Configuration Steps	● Define an address pool net172. ● The network segment is 172.16.1.0/24. ● The default gateway is 172.16.1.254. ● The address lease is 1 day. ● Excluded addresses range from 172.16.1.2 to 172.16.1.100.
	FS(config)# ip dhcp excluded-address 172.16.1.2 172.16.1.100 FS(dhcp-config)# ip dhcp pool net172 FS(dhcp-config)# network 172.16.1.0 255.255.255.0 FS(dhcp-config)# default-router 172.16.1.254 FS(dhcp-config)# lease 1

Verification	Run the **show run** command to display the configuration.
	FS(config)#show run | begin ip dhcp ip dhcp excluded-address 172.16.1.2 172.16.1.100 ip dhcp pool net172 network 172.16.1.0 255.255.255.0default-router 172.16.1.254 lease 1

3.4.2 Configuring Static IP Address

Configuration Effect

Assign specific IP addresses and push configuration to specific DHCP clients.

Notes

N/A

Configuration Steps

Configuring Address Pool Name and Entering Address Pool Configuration Mode

- Mandatory. It is used to create an IP address pool.
- Run the **ip dhcp pool** command in global configuration mode.

Configuring IP Address and Subnet Mask of Client

- Mandatory. It is used to configure a static IP address and a subnet mask.
- Run the **host** command in DHCP address pool configuration mode.

Configuring Hardware Address of Client

- Optional. It is used to configure a MAC address.
- Run the **hardware** command in DHCP address pool configuration mode.

Configures Unique Client Identifier

- Optional. It is used to configure a static user identifier (UID).
- Run the **client-identifier** command in DHCP address pool configuration mode.

Configuring Client Name

- Optional. It is used to configure a static client name.
- Run the **host-name** command in DHCP address pool configuration mode.

Verification

Check whether the client obtains the IP address when it is online.

Related Commands

Configuring Address Pool

Command	**ip dhcp pool** *dhcp-pool*
Parameter Description	*pool-name*: Indicates the name of an address pool.
Command Mode	Global configuration mode
Usage Guide	Before assigning an IP address to a client, you need to configure an address pool name and enter address pool configuration mode.

Manual IP Address Binding

Command	**host** *ip-address* [*netmask*] **client-identifier** *unique-identifier* **client-name** *name*
Parameter Description	*ip-address:* Defines the IP address of a DHCP client. *netmask:* Defines the subnet mask of a DHCP client. *unique-identifier:* Defines the hardware address (for example, aabb.bbbb.bb88) and identifier (for example, 01aa.bbbb.bbbb.88) of a DHCP client. *name:* (Optional) It defines a client name using ASCII characters. The name excludes a domain name. For example, name a host **mary** rather than **mary.fs.com**.
Command Mode	DHCP address pool configuration mode
Usage Guide	Address binding means mapping between an IP address and a client's MAC address. There are two kind of address binding. 1) Manual binding. Manual binding can be deemed as a special DHCP address pool with only one address. 2) Dynamic binding. A DHCP server dynamically assigns an IP address from a pool to a client when it receives a DHCP request, creating mapping between the IP address and the client's MAC address. To configure manual binding, you need to define a host pool and then specify a DHCP client's IP address and hardware address or identifier. A hardware address is a MAC address. A client identifier includes a network medium type and a MAC address. A Microsoft client is usually identified by a client identifier rather than a MAC address. For the codes of medium types, refer to the *Address Resolution Protocol Parameters* section in the RFC 1700. The Ethernet type is **01**.

Configuration Example

Dynamic IP Address Pool

Configuration Steps	● Configure address pool VLAN 1 with IP address 20.1.1.0 and subnet mask 255.255.255.0. ● The default gateway is 20.1.1.1. ● The lease time is 1 day.
	FS(config)# ip dhcp pool vlan1 FS(dhcp-config)# network 20.1.1.0 255.255.255.0 FS(dhcp-config)# default-router 20.1.1.1 FS(dhcp-config)# lease 1 0 0

Verification	● Run the **show run** command to display the configuration.
	FS(config)#show run | begin ip dhcp ip dhcp pool vlan1 network 20.1.1.0 255.255.255.0 default-router 20.1.1.1 lease 1 0 0

Manual Binding

Configuration Steps	● The host address is 172.16.1.101 and the subnet mask is 255.255.255.0. ● The host name is Billy.rg.com. ● The default gateway is 172.16.1.254. ● The MAC address is 00d0.df34.32a3.
	FS(config)# ip dhcp pool Billy FS(dhcp-config)# host 172.16.1.101 255.255.255.0 FS(dhcp-config)# client-name Billy FS(dhcp-config)# hardware-address 00d0.df34.32a3 Ethernet FS(dhcp-config)# default-router 172.16.1.254
Verification	Run the **show run** command to display the configuration.
	FS(config)#show run | begin ip dhcp ip dhcp pool Billy host 172.16.1.101 255.255.255.0 client-name Billy hardware-address 00d0.df34.32a3 Ethernet default-router 172.16.1.254

Alternative Configuration Steps

Configuring Address Pool Name and Entering Address Pool Configuration Mode

- Mandatory. It is used to create an IP address pool.
- Run the **ip dhcp pool** command in global configuration mode.

Binding a Static IP Address

- Mandatory. It is used to bind a static IP address.
- Run the **static-bind** command in DHCP address pool configuration mode.

3.4.3 Configuring Global Properties of DHCP Server

Configuration Effect

Enable a server with specific functions, for example, ping and compulsory NAK.

Notes

Configuring the command may cause exceptions on other servers.

Configuration Steps

Configuring Excluded IP Address

- Optional. Configure some addresses or address ranges as unavailable.
- Run the **ip dhcp excluded-address** command in global configuration mode.

Configuring Compulsory NAK Reply

- Optional. A server replies to a wrong address request with a NAK packet.
- Run the **ip dhcp force-send-nak** command in global configuration mode.

Configuring VRRP Status Monitoring

- Optional. After configuration, DHCP packets are processed by the Master server.
- Run the **ip dhcp monitor-vrrp-state** command in global configuration mode.

Configuring Ping Times

- Optional. Check the address reachability with the **ping** command. The default is 2.
- Run the **ip dhcp ping packet** command in global configuration mode.

Configuring Ping Timeout

- Optional. Check the address reachability with the **ping** command. The default is 500 ms.

Run the **ip dhcp ping timeout** command in global configuration mode.

Refreshing Trusted ARP

- Configure a DHCP server to refresh trusted ARPs according to the addresses assigned from an address pool configured with the **update arp** command.
- Run the **ip dhcp refresh arp** command in global configuration mode.

Configuring Pseudo Server Detection

- Optional. Enable this function to log a pseudo server.
- Run the **ip dhcp server detect** command in global configuration mode.

Verification

Run the dhcp-server command, and check the configuration during address assignment.

Related Commands

Configuring Excluded IP Address

Command	**ip dhcp excluded-address** *low-ip-address* [*high-ip-address*]
Parameter Description	*low-ip-address:* Indicates a start IP address. *high-ip-address:* Indicates an end IP address.
Command Mode	Global configuration mode
Usage Guide	Unless otherwise specified, a DHCP server assigns all the addresses from an IP address pool to DHCP clients. To reserve some addresses(e.g., addresses already assigned to the server or devices), you need to configure these addresses as excluded addresses. To configure a DHCP server, it is recommended to configure excluded addresses to avoid address conflict and shorten detection time during address assignment.

Configuring Compulsory NAK Reply

Command	**ip dhcp force-send-nak**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	In a WLAN, a DHCP client often moves from one network to another. When a DHCP server receives a lease renewal request from a client but finds that the client crosses the network segment or that the lease is expired, it replies with a NAK packet to require the client to obtain an IP address again. This prevents the client from sending request packets continually before obtaining an IP address again after timeout. The server sends a NAK packet only when it finds the client's lease record. When a DHCP client crosses the network, a DHCP server cannot find lease record of the client and will not reply with a NAK packet. The client sends request packets continually before obtaining an IP address again after timeout. Consequently, it takes a long to obtain an IP address. This also occurs when a DHCP server loses a lease after restart and a client requests lease renewal. In this case, you may configure a command to force the DHCP server to reply with a NAK packet even though it cannot find the lease record so that the client may obtain an IP address rapidly. Please note that the command is disabled by default. To enable it, only one DHCP server can be configured in a broadcast domain.

Configuring Ping Times

Command	**ip dhcp ping packets** [*number*]
Parameter Description	*number:* (Optional) Ranges from 0 to 10. 0 indicates the ping function is disabled. The default is two pings.
Command Mode	Global configuration mode
Usage Guide	By default, when a DHCP server assigns an IP address from a pool, it runs the **Ping** command twice (one packet per time). If there is no reply, the server takes the address as idle and assigns it to a client. If there is a reply, the server takes the address as occupied and assigns another address.

Configuring Ping Timeout

Command	**ip dhcp ping timeout** *milliseconds*
Parameter Description	*milli-seconds:* Indicates the time that it takes for a DHCP server to wait for a ping reply. The value ranges from 100 ms to 10,000 ms.
Command Mode	Global configuration mode
Usage Guide	By default, if a DHCP server receives no Ping reply within 500 ms, the IP address is available. You may adjust the ping timeout to change the time for a server to wait for a reply.

Refreshing Trusted ARP

Command	**ip dhcp refresh arp**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, if an address pool is configured with the **update arp** command, a DHCP server will refresh trusted ARPs while assigning an IP address from the address pool. If a client clears the trusted ARPs, the server will not reassign them. After configuration, a DHCP server may refresh trusted ARPs according to addresses assigned from an address pool configured with **update arp**.

Configuring Pseudo Server Detection

Command	**ip dhcp server detect**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, pseudo server detection is disabled on a DHCP server. Run this command to enable pseudo server detection.

Configuration Example

Configuring Ping

Configuration Steps	• Set ping times to 5. • Set ping timeout to 800ms.
	FS(config)# ip dhcp ping packet 5 FS(config)# ip dhcp ping timeout 800
Verification	Run the **show run** command to display the configuration.
	FS(config)#show run | begin ip dhcp ip dhcp ping packet 5 ip dhcp ping timeout 800

Configuring Excluded IP Address

Configuration Steps	● Configure the excluded IP address from 192.168.0.0 to 192.168.255.255.
	FS(config)# ip dhcp excluded-address 192.168.0.0 192.168.255.255
Verification	Run the **show run** command to display the configuration.
	FS(config)#show run | begin ip dhcp ip dhcp excluded-address 192.168.0.0 192.168.255.255

3.4.4 Configuring Basic DHCP Relay Functions

Configuration Effect

- Deploy dynamic IP management in Client–Relay–Server mode to achieve communication between a DHCP client and a DHCP server, which are in different network segments.

Notes

- To enable DHCP Relay, you need to configure IPv4 unicast routing in a network.

Configuration Steps

Enabling DHCP Relay

- Mandatory.
- Unless otherwise specified, you need to enable DHCP Relay on a device.

Configuring IP Address for DHCP Server

- Mandatory.
- You need to configure an IP address for a DHCP server.

Verification

- Check whether a client obtains an IP address through DHCP Relay.

Related Commands

Enabling DHCP Relay

Command	service dhcp
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring IP Address for DHCP Server

Command	**ip helper-address { cycle-mode | *A.B.C.D* }**
Parameter Description	*cycle-mode*: Indicates that DHCP request packets are forwarded to all DHCP servers. *A.B.C.D*: Indicates the IP address of a server.
Command Mode	Global configuration mode/interface configuration mode
Usage Guide	You may configure the function on a layer-3 interface, such as a routed port, a L3 AP port, SVI and loopback interface. The configured interface must be accessible via IPv4 unicast routing.

Configuration Example

Configuring DHCP Relay in Wired Connection

Scenario Figure 2-10	
Configuration Steps	● Enable a client with DHCP to obtain an IP address. ● Enable the DHCP Relay function on a DHCP relay agent. ● Configure DHCP Server.
A	Enable a client with DHCP to obtain an IP address.
B	Enable DHCP Relay. FS(config)# service dhcp Configure a global IP address of a DHCP server. FS(config)# ip helper-address 172.2.2.1 Configure an IP address for the port connected to the client. FS(config)# interface gigabitEthernet 0/1 FS(config-if)# ip address 192.1.1.1 255.255.255.0 Configure an IP address for the port connected to the server. FS(config)# interface gigabitEthernet 0/2 FS(config-if-gigabitEthernet 0/2)# ip address 172.2.2.2 255.255.255.0
C	Enable DHCP Server. FS(config)# service dhcp Configure an address pool. FS(config)# ip dhcp pool relay FS (dhcp-config)#network 192.1.1.0 255.255.255.0

	FS (dhcp-config)#default-router 192.1.1.1 Configure an IP address for the port connected to the relay agent. FS(config)# interface gigabitEthernet 0/1 FS(config-if-gigabitEthernet 0/2)# ip address 172.2.2.1 255.255.255.0
Verification	Check whether the client obtains an IP address. ● Check whether the client obtains an IP address. ● Check the DHCP Relay configuration.
A	The user device obtains an IP address.
B	After login to the DHCP relay agent, run the **show running-config** command in privileged EXEC mode to display DHCP Relay configuration. FS# show running-config service dhcp ip helper-address 172.2.2.1 ! interface GigabitEthernet 0/1 ip address 192.1.1.1 255.255.255.0 ! interface GigabitEthernet 0/2 ip address 172.2.2.2 255.255.255.0 !

Common Errors

- IPv4 unicast routing configuration is incorrect.
- DHCP Relay is disabled.
- No routing between DHCP relay agent and DHCP server is configured.
- No IP address is configured for the DHCP server.

3.4.5 Configuring DHCP Relay Option 82

Configuration Effect

- Through a DHCP relay agent, a server may assign IP addresses of different privileges to the clients more accurately based on the option information.

Notes

- You need to enable the DHCP Relay function.

Configuration Steps

Enabling Basic DHCP Relay Functions

- Mandatory.
- Unless otherwise specified, you need to enable DHCP Relay on a device.

Enables DHCP Option82

- By default, DHCP Option 82 is disabled.
- You may run the **ip dhcp relay information option82 [standard-format | verbose-format]** command to enable or disable DHCP Option 82.

3.4.6 Configuring DHCP Client

Configuration Effect

Enable DHCP Client on a device so that it obtains IP addresses and configurations dynamically.

Notes

FS products support DHCP Client configuration on Ethernet, FR, PPP and HDLC interfaces.

Configuration Steps

Run the ip address dhcp command on an interface.

Verification

Check whether the interface obtains an IP address.

Related Commands

Configuring DHCP Client

Command	ip address dhcp
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	● FS products support dynamic IP address obtainment by an Ethernet interface. ● FS products support dynamic IP address obtainment by a PPP-encapsulated interface. ● FS products support dynamic IP address obtainment by an FR-encapsulated interface. ● FS products support dynamic IP address obtainment by an HDLC-encapsulated interface.

Configuration Example

Configuring DHCP Client

Configuration	1: Enable port FastEthernet 0/0 with DHCP to obtain an IP address.

Steps	
	FS(config)# interface FastEthernet0/0 FS(config-if-FastEthernet 0/0)#ip address dhcp
Verification	1: Run the **show run** command to display the configuration.
	FS(config)#show run | begin ip address dhcp ip address dhcp

3.4.7 Assigning Static IP Addresses

Configuration Effect

Assign a static IP address to a specified access location, terminal, and terminal host name.

Notes

1. The access location can be obtained only when a FS access switch serves as a terminal.
2. The access location and host name may conflict. As a result, they cannot uniquely identify a terminal. In this case, a static IP address cannot be bound to the location and host name.

Configuration Steps

Binding a Static IP Address to Specified Information

- Run the **ip dhcp add-client** command in global configuration mode.

Verification

Run the show run command to check whether the configuration is successful.

Related Commands

Binding and Assigning a Static IP Address to Specified Information

Command	**ip dhcp add-client { solidify-ip ip** *ip-addr* **{ { access-device** *dev-addr* **access-vlan** *vlanid* **access-port** *portid* **| host-name** *hostname* **| mac** *mac-addr* **} binding-type { ip-hostname | ip-hostname-location | ip-mac | ip-mac-hostname | ip-mac-hostname-location | ip-mac-location } } | solidify-location ip** *ip-addr* **access-device** *dev-addr* **access-vlan** *vlanid* **access-port** *portid* **| solidify-mac mac** *mac-addr* **}**
Parameter Description	*Binding-type*: Indicates the binding type of a static IP address. A static IP address can be bound and assigned to different combinations of the access location, terminal host name, and terminal MAC address. *Ip-addr*: Indicates the assigned and bound static IP address. *Dev-addr*: Indicates the IP address or MAC address of the access device. *Vlanid*: Indicates the ID of the VLAN, to which the port connected to the terminal belongs. *Portid*: Indicates the port ID of the device, to which the terminal is connected.

	hostname: Indicates the terminal host name. *mac-addr*: Indicates the terminal MAC address.
Command Mode	Configuration mode
Usage Guide	This command is configured on the server to assign a static IP address based on any or any combination of a specified access location, host name, and terminal MAC address. Bound information of a static IP address is also used for authorized address assignment. When the authorized address assignment mode is enabled for an address pool, an IP address is assigned to a terminal only after the terminal hits the bound information.. For terminals with only the MAC addresses bound, this configuration is available only in authorized address assignment mode. In other modes, the IP addresses are normally and dynamically assigned.

Configuration Example

Assigning a Static IP Address to a Specified Terminal MAC Address

Configuration Steps	1. Assign the static IP address 192.168.100.100 to a terminal with the MAC address of 0000.dddd.eeee.
	FS(config)# ip dhcp add-client solidify-ip 192.168.100.100 mac 0000.dddd.eeee binding-type ip-mac
Verification	Run the **show run** command to check whether the configuration is successful.
	FS(config)#sh run | in solidify ip dhcp add-client solidify-ip 192.168.100.100 mac 0000.dddd.eeee binding-type ip-mac

3.5 Monitoring

Clearing

Running the clear commands may lose vital information and interrupt services.

Description	Command
Clears DHCP address binding.	**clear ip dhcp binding** { *address* | *}
Clears DHCP address conflict.	**clear ip dhcp conflict** { *address* | *}
Clears statistics of a DHCP server.	**clear ip dhcp server statistics**
Clears statistics of a DHCP relay.	**clear ip dhcp relay statistics**
Clears statistics of DHCP server performance.	**clear ip dhcp server rate**
Clears information of a DHCP pseudo server.	**clear ip dhcp server detect**
Clears entries of DHCP clients to be authorized.	**clear ip dhcp auth-agent**

Clears dynamic online DHCP entries.	**clear ip dhcp dynamic-binding**
Clears online DHCP history statistics information.	**clear ip dhcp record-history**
Clears	**clear ip dhcp solid-binding**
Clears DHCP service warning logs.	**clear ip dhcp warn-log**

Displaying

Description	Command
Displays DHCP lease.	**show dhcp lease**
Displays DHCP sockets.	**show ip dhcp socket**
Displays assigned IP addresses.	**show ip dhcp binding**
Displays created address pools.	**show ip dhcp pool**
Displays statistics of DHCP Server.	**show ip dhcp server statistic**
Displays statistics of DHCP Relay.	**show ip dhcp relay statistic**
Displays conflicted addresses.	**show ip dhcp conflict**
Displays the DHCP pseudo server.	**show ip dhcp server detect**
Displays the DHCP server state, number of warning logs and authentication information.	**show dhcp state**
Displays details of all address pools.	**show dhcp all-pool json**
Displays details of the sorted address pools.	**show ip dhcp sort-pool status**
Displays details of online IP addresses.	**show ip dhcp online-agent x.x.x.x**
Displays the configuration of user logs.	**show ip dhcp agent-log json**
Displays the DHCP clients to be authorized.	**show ip dhcp auth-agent json**
Displays details of warning logs.	**show ip dhcp warn-log {address-conflict | address-shift | hist-addr-cflt | hist-addr-shift | hist-pool-exhaust | pool-exhaust | statistic }**
Displays security binding information.	**show ip dhcp safe-bind**
Displays details of historical online records.	**show ip dhcp record-history json**
Displays information of online addresses.	**show ip dhcp history [detail]**
Displays the usage state of all address pools.	**show ip dhcp all-pool {stat | order {more-pool | used-number | used-percent}}**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs DHCP agent.	**debug ip dhcp server agent**
Debugs DHCP hot backup.	**debug ip dhcp server ha**
Debugs DHCP address pools.	**debug ip dhcp server pool**
Debugs DHCP VRRP.	**debug ip dhcp server vrrp**
Debugs all DHCP servers.	**debug ip dhcp server all**
Debugs DHCP packets.	**debug ip dhcp client**
Debugs DHCP Relay events.	**debug ip dhcp relay**

4 Configuring DNS

4.1 Overview

A Domain Name System (DNS) is a distributed database containing mappings between domain names and IP addresses on the Internet, which facilitate users to access the Internet without remembering IP strings that can be directly accessed by computers. The process of obtaining an IP address through the corresponding host name is called domain name resolution (or host name resolution).

Protocols and Standards

- RFC1034: DOMAIN NAMES - CONCEPTS AND FACILITIES
- RFC1035: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

4.2 Applications

Application	Description
Static Domain Name Resolution	Performs domain name resolution directly based on the mapping between a domain name and an IP address on a device.
Dynamic Domain Name Resolution	Obtains the IP address mapped to a domain name dynamically from a DNS server on the network.

4.2.1 Static Domain Name Resolution

Scenario

- Preset the mapping between a domain name and an IP address on a device.
- When you perform domain name operations (such as Ping and Telnet) through application programs, the system can resolve the IP address without being connected to a server on the network.

Deployment

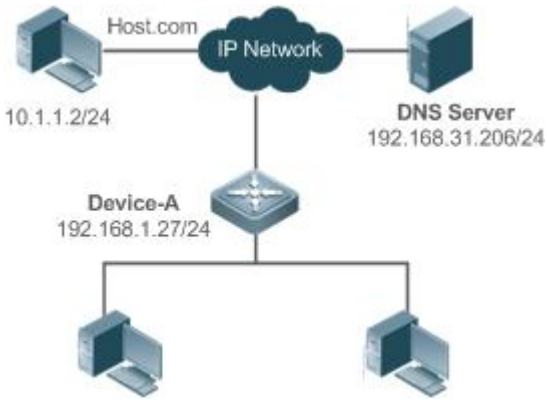
- Preset the mapping between a domain name and an IP address on a device.

4.2.2 Dynamic Domain Name Resolution

Scenario

- DNS Server is deployed on the network to provide the domain name service.
- Domain name "host.com" is deployed on the network.
- Device-A applies to DNS Server for domain name "host.com".

Figure 3-1 Dynamic Domain Name Resolution



Deployment

- Deploy DNS Server as the DNS server of Device-A.

4.3 Features

Basic Concepts

↘ DNS

The DNS consists of a resolver and a DNS server. The DNS server stores the mappings between domain names and IP addresses of all hosts on the network, and implements mutual conversion between the domain names and IP addresses. Both the TCP and UDP port IDs of DNS are 53, and generally a UDP port is used.

Features

Feature	Description
Domain Name Resolution	IP addresses are obtained based on domain names from a DNS server or a local database.

4.3.1 Domain Name Resolution

Working Principle

↘ Static Domain Name Resolution

Static domain name resolution means that a user presets the mapping between a domain name and an IP address on a device. When you perform domain name operations (such as Ping and Telnet) through application programs, the system can resolve the IP address without being connected to a server on the network.

↘ Dynamic Domain Name Resolution

Dynamic domain name resolution means that when a user perform domain name operations through application programs, the DNS resolver of the system queries an external DNS server for the IP address mapped to the domain name.
The procedure of dynamic domain name resolution is as follows:

4. A user application program (such as Ping or Telnet) requests the IP address mapped to a domain name from the DNS resolver of the system.
5. The DNS resolver queries the dynamic cache at first. If the domain name on the dynamic cache does not expire, the DNS resolver returns the domain name to the application program.

6. If all domain names expire, the DNS resolver initiates a request for domain name-IP address conversion to the external DNS server.
7. After receiving a response from the DNS server, the DNS resolver caches and transfers the response to the application program.

Related Configuration

Enabling Domain Name Resolution

- By default, domain name resolution is enabled.
- Run the **ip domain-lookup** command to enable domain name resolution.

Configuring the IP Address Mapped to a Static Domain Name

- By default, no mapping between a domain name and an IP address is configured.
- Run the **ip host** command to specify the IPv4 address mapped to a domain name.

Configuring a DNS Server

- By default, no DNS server is configured.
- Run the **ip name-server** command to configure a DNS server.

4.4 Configuration

Configuration	Description and Command	
Configuring Static Domain Name Resolution	Optional.	
	ip domain-lookup	Enables domain name resolution.
	ip host	Configures the IPv4 address mapped to a domain name.
Configuring Dynamic Domain Name Resolution	Optional.	
	ip domain-lookup	Enables domain name resolution.
	ip name-server	Configures a DNS server.

4.4.1 Configuring Static Domain Name Resolution

Configuration Effect

The system resolver resolves the IP address mapped to a domain name on a local device.

Configuration Steps

Enabling Domain Name Resolution

- The domain name resolution function is enabled by default.
- If this function is disabled, static domain name resolution does not take effect.

Configuring the IP Address Mapped to a Domain Name

- (Mandatory) Domain names to be used must be configured with mapped IP addresses.

Verification

- Run the **show run** command to check the configuration.
- Run the **show hosts** command to check the mapping between the domain name and the IP address.

Related Commands

Configuring the IPv4 Address Mapped to a Domain Name

Command	**ip host** *host-name ip-address*
Parameter Description	*host-name*: indicates a domain name. *ip-address*: indicates a mapped IPv4 address.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring Static Domain Name Resolution

Configuration Steps	● Set the IP address of static domain name www.test.com to 192.168.1.1 on a device.
	FS#configure terminal FS(config)# ip host www.test.com 192.168.1.1 FS(config)# exit
Verification	Run the **show hosts** command to check whether the static domain name entry is configured.
	FS#show hosts Name servers are: Host type Address TTL(sec) www.test.com static 192.168.1.1 ---

4.4.2 Configuring Dynamic Domain Name Resolution

Configuration Effect

The system resolver resolves the IP address mapped to a domain name through a DNS server.

Configuration Steps

Enabling Domain Name Resolution

- Domain name resolution is enabled by default.
- If this function is disabled, dynamic domain name resolution does not take effect.

Configuring a DNS Server

- (Mandatory) To use dynamic domain name resolution, you must configure an external DNS server.

Verification

- Run the **show run** command to check the configuration.

Related Commands

Configuring a DNS Server

Command	**ip name-server** [**oob**] { *ip-address* }
Parameter Description	*ip-address*: indicates the IPv4 address of the DNS server. **oob**: indicates that the DNS server supports an out-of-band management interface (interface of mgmt).
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring Dynamic Domain Name Resolution

Scenario Figure 3-2	
	Device resolves the domain name through the DNS server (192.168.10.1) on the network.
Configuration Steps	Set the IP address of the DNS server to 192.168.10.1 on the device.
	DEVICE#configure terminal DEVICE(config)# ip name-server 192.168.10.1 DEVICE(config)# exit
Verification	Run the **show hosts** command to check whether the DNS server is specified.
	FS(config)#show hosts Name servers are: 192.168.10.1 static

	Host type Address TTL(sec)

4.5 Monitoring

Clearing

Running the **clear** command during device operation may cause data loss or even interrupt services.

Description	Command
Clears the dynamic host name cache table.	**clear host** [*host-name*]

Displaying

Description	Command
Displays DNS parameters.	**show hosts** [*host-name*]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the DNS function.	**debug ip dns**

5 Configuring DDNS

5.1 Overview

The Dynamic Domain Name Server (DDNS) maps a dynamic IP address to a fixed domain name resolution server. When accessing the network, a client program sends the dynamic IP address of the host to the server program located in a host of the service provider. The server program provides the domain name service (DNS) and implements dynamic domain name resolution.

The DDNS binds a dynamic public IP address allocated by the Internet service provider (ISP) to a device to a domain name. For a client that uses a dynamic IP address for access, the DDNS binds the dynamic IP address to a fixed domain name, and maps an internal service to the public network. Therefore, a service provided by the ISP can be accessed in the Internet via the fixed domain name.

At present, FS gateways support the DDNS provided by Oray and 3322. The following merely describes information related to the DDNS provided by Oray and 3322.

5.2 Applications

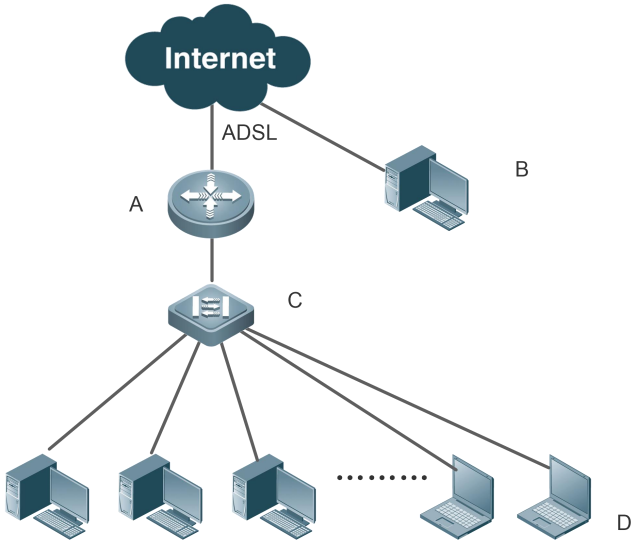
Application	Description
Deploying Dynamic Dialup Egress Gateway	The DDNS is deployed in a dynamic dialup egress environment.

5.2.1 Deploying Dynamic Dialup Egress Gateway

Scenario

In some small cybercafé, a gateway dials up to access the network and serves as a DDNS client to register an IP address with the DDNS server.

Figure 4-1



Remarks	A is an egress gateway. B is a DDNS server provided by Oray or 3322. C is a switch. D are clients accessing the network.

Deployment

- Dial up from an internal network to access the Internet.
- Use the egress gateway as a DDNS client to register an IP address with the DDNS server.
- Access the egress gateway from an external network via the dynamic domain name.

5.3 Features

Overview

Feature	Description
Connecting to DDNS Server	Connects to the DDNS server, verify the username and password, and bind the device IP address to the domain name.

5.3.1 Connecting to DDNS Server

Connect to DDNS server, verify the username and password, and bind the device IP address to the domain name.

Working Principle

Based on the implementation of the DDNS client protocol, the egress gateway serves as the DDNS client to provide DDNS services to users.

5.4 Configuration

Configuration	Description and Command	
Configuring DDNS Account and Password	(Mandatory) It is used to connect to the DDNS server, verify the username and password, and bind the device IP address to the domain name.	
	ddns service *service* [**domain** *domain*] **username** *username* **password** *password* **service** *service* [**interface** *interface-name*]	Configures the username and password, and binds an interface.

5.4.1 Configuring DDNS Account and Password

Configuration Effect

- Connect to the DDNS server, verify the username and password, and bind the device IP address to the domain name.

Configuration Steps

Configuring DDNS Account and Password

- Mandatory. No DDNS account and password are configured by default.
- After the DDNS account and password are configured, the device immediately initiates a connection to the DDNS server, verify the account and password, and bind the device IP address to the domain name.

Command	**ddns service** *service* [**domain** *domain*] **username** *username* **password** *password* **service** *service* [**interface** *interface-name*]
Parameter Description	*service:* Indicates the DDNS provider, Oray.org or 3322.org. *domain:* Indicates the 3322.org. It is used only for the 3322.org service. *username*: Indicates the DDNS account. *password*: Indicates the DDNS password. *interface-name:* Indicates the external interface.
Defaults	No interface is bound.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

Display the DDNS status of the device.

Command	**show ddns**
Parameter Description	N/A

Command Mode	Privileged EXEC mode and global configuration mode
Usage Guide	Use this command to display the DDNS status.
Command Presentation	FS#show ddns ----------[0]---------- status: Success code: none service: oray username: FS password: FS domain: FS.imwork.net interface: Gi0/7 ----------[1]---------- status: Success code: good service: 3322 username: FS password: FS domain: FS.f3322.net interface:

For details about the **show** command, see the command manual of corresponding feature.

Configuration Example

Configuring DDNS Account and Password

Configuration Steps	● Configure the DDNS account, password and bound interface.
A	FS#configure terminal FS (config)# ddns service oray username FS password FS interface GigabitEthernet 0/7 FS (config)# ddns service 3322 domain FS.f3322.net username FS password FS interface GigabitEthernet 0/7
Verification	● Run the **show ddns** command to display the DDNS status.
A	FS#show ddns ----------[0]---------- status: Success code: none service: oray username: FS password: FS domain: FS.imwork.net interface: Gi0/7 ----------[1]----------

	status: Success code: good service: 3322 username: FS password: FS domain: FS.f3322.net interface:

Common Errors

- The DDNS account or password is incorrect.
- The DNS is incorrectly configured in the device, leading to the failure in resolving the IP address of the DDNS server.
- The DDNS server is unreachable.

5.5 Monitoring

Displaying

Description	Command
Displays the DDNS status of the device.	**show ddns**

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs the DDNS process.	**debug ddns proc**
Debugs the DDNS service.	**debug ddns all**
Debugs the Oray service.	**debug ddns oray**
Debugs the 3322 service.	**debug ddns pubyun**

6 Configuring NTP

6.1 Overview

The Network Time Protocol (NTP) is an application-layer protocol that enables network devices to synchronize time. NTP enables network devices to synchronize time with their servers or clock sources and provides high-precision time correction (the difference from the standard time is smaller than one millisecond in a LAN and smaller than decades of milliseconds in a WAN). In addition, NTP can prevent attacks by using encrypted acknowledgment.

Currently, FS devices can be used both as NTP clients and NTP servers. In other words, a FS device can synchronize time with a time server, and be used as a time server to provide time synchronization for other devices. When a FS device is used as a server, it supports only the unicast server mode.

Protocols and Standards

- RFC 1305 : Network Time Protocol (Version 3)

6.2 Applications

Application	Description
Synchronizing Time Based on an External Reference Clock Source	A device is used as a client that synchronizes time with an external clock source. After successful synchronization, it is used as a server to provide time synchronization for other devices.
Synchronizing Time Based on a Local Reference Clock Source	A device uses a local clock as a reliable NTP reference clock source and is also used as a server to provide time synchronization for other devices.

6.2.1 Synchronizing Time Based on an External Reference Clock Source

Scenario

As shown in Figure 5-1:

- DEVICE-A is used as a reliable reference clock source to provide time synchronization for external devices.
- DEVICE-B specifies DEVICE-A as the NTP server and synchronizes time with DEVICE-A.
- After successful synchronization, DEVICE-B provides time synchronization for DEVICE-C.

Figure 5-1

Deployment

Configure DEVICE-B to the NTP external reference clock mode.

6.2.2 Synchronizing Time Based on a Local Reference Clock Source

Scenario

As shown in Figure 5-2, DEVICE-B uses a local clock as the NTP reference clock source and provides time synchronization for DEVICE-C.

Figure 5-2

Deployment

Configure DEVICE-B to the NTP local reference clock mode.

6.3 Features

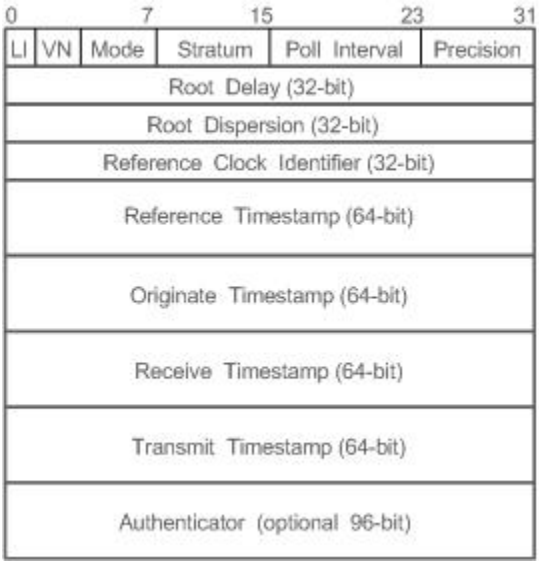
Basic Concepts

NTP Packet

As defined in RFC1305, NTP uses User Datagram Protocol (UDP) packets for transmission and the used UDP port ID is 123.

Figure 5-3 shows the format of an NTP time synchronization packet.

Figure 5-3 Format of an NTP Time Synchronization Packet



- Leap Indicator(LI): indicates a 2-bit leap second indicator.

00: indicates no warning information; 01: indicates that there are 61 seconds in the previous minute; 10: indicates that there are 59 seconds in the previous minute; 11: indicates that the clock is not synchronized.

- Version Number(VN): indicates a 3-bit NTP version number. The current version number is 3.
- Mode: indicates a 3-bit NTP working mode.

0: indicates no definition; 1: indicates symmetric active; 2: indicates symmetric passive; 3: indicates a client; 4: indicates a server; 5: indicates broadcasting; 6: indicates control information; 7: reserved.

- Stratum: indicates the 8-bit stratum of a local clock. 0: indicates no definition; 1: indicates the master reference clock source; other values: indicate slave reference clock sources.
- Poll Interval: indicates the poll interval (seconds), which is a 8-bit integer.

- Precision: indicates the time precision (seconds) of a local clock, which is a 8-bit integer.
- Root Delay: indicates the round-trip time to the master reference clock source, which is a 32-bit integer.
- Root Dispersion: indicates the largest difference from the master reference clock source, which is a 32-bit integer.
- Reference Clock Identifier: indicates the 32-bit identifier of a reference clock source.
- Reference Timestamp: indicates a 64-bit timestamp, namely, the time that is set or corrected at the last time.
- Originate Timestamp: indicates a 64-bit timestamp, namely, the local time when a time synchronization request leaves from a client.
- Receive Timestamp: indicates a 64-bit timestamp, namely, the local time when a time synchronization request packet arrives at a server.
- Transmit Timestamp: indicates a 64-bit timestamp, namely, the local time when a time synchronization response packet leaves from a server.
- Authenticator (optional): indicates authentication information.

NTP Server

A device uses a local clock as the reference clock source to provide time synchronization for other devices in the network.

NTP Client

A device is used as an NTP client that synchronizes time with an NTP server in the network.

Stratum

In NTP, "stratum" is used to describe the hops from a device to an authority clock source. An NTP server whose stratum is 1 has a directly connected atomic clock or radio controlled clock; an NTP server whose stratum is 2 obtains time from the server whose stratum is 1; an NTP server whose stratum is 3 obtains time from the server whose stratum is 2; and so on. Therefore, clock sources with lower stratums have higher clock precisions.

Hardware Clock

A hardware clock operates based on the frequency of the quartz crystal resonator on a device and is powered by the device battery. After the device is shut down, the hardware clock continues running. After the device is started, the device obtains time information from the hardware clock as the software time of the device.

Overview

Feature	Description
NTP Time Synchronization	Network devices synchronize time with their servers or reliable clock sources to implement high-precision time correction.
NTP Security Authentication	The NTP packet encryption authentication is used to prevent unreliable clock sources from time synchronization interference on a device.
NTP Access Control	An Access Control List (ACL) is used to filter sources of received NTP packets.

6.3.1 NTP Time Synchronization

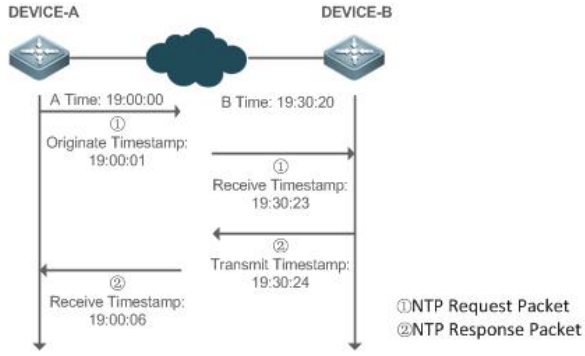
Working Principle

NTP time synchronization is implemented by interaction of NTP packets between a client and a server:

- The client sends a time synchronization packet to all servers every 64 seconds. After receiving response packets from the servers, the client filters and selects the response packets from all servers, and synchronizes time with an optimum server.
- After receiving the time synchronization request packet, a server uses the local clock as the reference source, and fills the local time information into the response packet to be sent to the client based on the protocol requirement.

Figure 5-4 shows the format of an NTP time synchronization packet.

Figure 5-4 Working Principle of NTP



DEVICE-B (B for short) is used as an NTP reference clock source, DEVICE-A (A for short) is used as an NTP client that synchronizes time with DEVICE-B. At a time point, the local clock of A is 19:00:00 and the local clock of B is 19:30:20.

8. A sends an NTP request packet. The local time (T0) when the packet leaves from A is 19:00:00 and is filled in Originate Timestamp.
9. After a 2-second network delay, the local time (T1) when B receives the request packet is 19:30:23 and is filled in Receive Timestamp.
10. B processes the NTP request and sends an NTP response packet one second later. The local time (T2) when the response packet leaves from B is 19:30:24 and is filled in Transmit Timestamp.
11. After a 2-second network delay, A receives the response packet. The local time (T3) when the response packet arrives at A is 19:00:06.

The specific calculations for time synchronization are as follows:

- A obtains the time difference of 30 minutes and 20 seconds between B and A by using the formula ((T1-T0)+(T2-T3))/2.
- A obtains the packet round-trip delay of four seconds between A and B by using the formula (T3-T0)-(T2-T1).

NTP Working Mode

- External clock reference mode

In this mode, a device is used as both a server and a client. If receiving time synchronization requests from other clients, the device must synchronize time with the specified server first and provide time synchronization for the clients after successful synchronization.

- Local clock reference mode

In this mode, a device uses the default local clock as the reliable clock source and provides time synchronization directly for other clients.

Related Configuration

Configuring an NTP Server

- The NTP function is disabled by default.

- Run the **ntp server** command to specify an NTP server (external clock reference source), which can enable NTP.
- After the configuration, the device works in the external clock reference mode.

Real-time Synchronization

- A device performs time synchronization every 64 seconds by default.

Updating a Hardware Clock

- By default, a device does not update synchronized time to the hardware clock.
- Run the **ntp update-calendar** command to enable a device to automatically update the hardware clock after successfully synchronizing time each time.

Configuring the NTP Master Clock

- By default, a device works in the external clock reference mode.
- Run the **ntp master** command to configure a device to the local clock reference mode.

6.3.2 NTP Security Authentication

To prevent malicious damage on an NTP server, NTP uses the authentication mechanism to check whether the time synchronization information is really from the announced server and check the information return path to provide an anti-interference protection mechanism.

Working Principle

An NTP client and an NTP server are configured with the same key. When sending request and response packets, a device calculates the hash values of the packets by using the MD5 algorithm based on the specified key and NTP packet content, and fills the hash values into the packet authentication information. The receiving device checks whether the packets are sent by a trusted device or modified based on the authentication information.

Related Configuration

Configuring a Global Security Authentication Mechanism for NTP

- By default, no NTP security authentication mechanism is enabled.
- Run the **ntp authenticate** command to enable the NTP security authentication mechanism.

Configuring a Global Authentication Key for NTP

- By default, no global authentication key is configured.
- Run the **ntp authentication-key** command to enable an NTP global authentication key.

Configuring a Globally Trusted Key ID for NTP

- By default, no globally trusted key is configured.
- Run the **ntp trusted-key** command to configure a device as the reference clock source to provide a trusted key for time synchronization externally.

Configuring a Trusted Key ID for an External Reference Clock Source

- Run the **ntp server** command to specify an external reference source and the trusted key of this clock source as well.

6.3.3 NTP Access Control

Working Principle

Provide a minimum security measure by using an ACL.

Related Configuration

Configuring the Access Control Rights for NTP Services

- By default, there is no access control right for NTP.
- Run the **ntp access-group** command to configure the access control rights for NTP.

6.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions of NTP	(Mandatory) It is used to enable NTP. After NTP is enabled, a device works in the external clock reference mode.	
	ntp server	Configures an NTP server.
	ntp update-calendar	Automatically updates a hardware clock.
	(Optional) It is used to configure a device to the local clock reference mode.	
	ntp master	Configures the NTP master clock.
	(Optional) It is used to disable NTP.	
	no ntp	Disables all functions of NTP and clears all NTP configurations.
	ntp disable	Disables receiving of NTP packets from a specified interface.
Configuring NTP Security Authentication	(Optional) It is used to prevent unreliable clock sources from performing time synchronization interference on a device.	
	ntp authenticate	Enables a security authentication mechanism.
	ntp authentication-key	Configures a global authentication key.
	ntp trusted-key	Configures a trusted key for time synchronization.
	ntp server	Configures a trusted key for an external reference clock source.
Configuring NTP Access Control	(Optional) It is used to filter the sources of received NTP packets.	

	ntp access-group	Configures the access control rights for NTP.

6.4.1 Configuring Basic Functions of NTP

Configuration Effect

External Clock Reference Mode

- Use a device as a client to synchronize time from an external reference clock source to the local clock.
- After the time synchronization is successful, use the device as a time synchronization server to provide time synchronization.

Local Clock Reference Mode

- Use the local clock of a device as the NTP reference clock source to provide time synchronization.

Notes

- In the client/server mode, a device can be used as a time synchronization server to provide time synchronization only after successfully synchronizing time with a reliable external clock source.
- Once the local clock reference mode is configured, the system will not synchronize time with a clock source with a higher stratum.
- Configuring a local clock as the master clock (especially when specifying a lower stratum) may overwrite an effective clock source. If this command is used for multiple devices in a network, the clock difference between the devices may cause unstable time synchronization of the network.
- Before a local clock is configured as the master clock, if the system never synchronizes time with an external clock source, you may need to manually calibrate the system clock to ensure that there is no excessive difference. For details about how to manually calibrate the system clock, refer to the system time configuration section in the configuration guide.

Configuration Steps

Configuring an NTP Server

- (Mandatory) At least one external reference clock source must be specified (A maximum of 20 different external reference clock sources can be configured).
- If it is necessary to configure an NTP key, you must configure NTP security authentication before configuring the NTP server.

Automatically Updating a Hardware Clock

- Optional.
- By default, the system updates only the system clock, but not the hardware clock after successful time synchronization.
- After this command is configured, the system automatically updates the hardware clock after successful time synchronization.

Configuring the NTP Master Clock

- To switch a device to the local clock reference mode, run this command.

Disabling NTP

- To disable NTP and clear NTP configurations, run the **no ntp** command.

- By default, all interfaces can receive NTP packets after NTP is enabled. To disable NTP for a specified interface, run the **ntp disable** command.

Verification

- Run the **show ntp status** command to display the NTP configuration.
- Run the **show clock** command to check whether time synchronization is completed.

Related Commands

Configuring an NTP Server

Command	**ntp server**[**oob**]{ *ip-addr* / *domain* / **ip** *domain* }[**version** *version*][**source** *if-name*][**key** *keyid*][**prefer**]
Parameter Description	**oob**: Indicates whether a reference clock source is bound to the MGMT interface. *ip-addr*: Indicates the IPv4/IPv6 address of the reference clock source. *domain*: Indicates the IPv4/IPv6 domain name of the reference clock source. *version*: Indicates the NTP version number, ranging from 1 to 3. *if-name*: Indicates the interface type, including AggregatePort, Dialer GigabitEthernet, Loopback, Multilink, Null, Tunnel, Virtual-ppp, Virtual-template and Vlan. *keyid*: Indicates the key used for communicating with the reference clock source, ranging from 1 to 4294967295. **prefer**: Indicates whether the reference clock source has a high priority.
Command Mode	Global configuration mode
Usage Guide	By default, no NTP server is configured. FS client system supports interaction with up to 20 NTP servers. You can configure an authentication key for each server (after configuring global authentication and the related key) to initiate encrypted communication with the servers. If it is necessary to configure an authentication key, you must configure NTP security authentication before configuring an NTP server. The default version of NTP for communicating with a server is NTP version 3. In addition, you can configure the source interface for transmitting NTP packets and specify that the NTP packets from a corresponding server can be received only on the transmitting interface.

Updating a Hardware Clock

Command	**ntp update-calendar**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring a Local Reference Clock Source

Command	**ntp master**[*stratum*]
Parameter Description	*stratum*: specifies the stratum of a local clock, ranging from 1 to 15. The default value is 8.
Command Mode	Global configuration mode
Usage Guide	N/A

Disabling NTP

Command	**no ntp**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This command can be used to fast disable all functions of NTP and clear all NTP configurations.

Disabling Receiving of NTP Packets on an Interface

Command	**ntp disable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

External Clock Reference Mode of NTP

Scenario Figure 5-5	
	● DEVICE-B is configured to the NTP external clock reference mode. ● DEVICE-A is used as the reference clock source of DEVICE-B. ● DEVICE-C synchronizes time with DEVICE-B.
Configuration Steps	● DEVICE-A configures the local clock as the NTP reference clock source. ● DEVICE-B configures DEVICE-A as the reference clock source. ● DEVICE-C configures DEVICE-B as the reference clock source.
DEVICE-A	A#configure terminal

	A(config)# ntp master A(config)#exit
DEVICE-B	B#configure terminal B(config)# ntp server 192.168.1.1 B(config)# exit
DEVICE-C	C#configure terminal C(config)# ntp server 192.168.2.1 C(config)# exit
Verification	● Run the **show ntp status** command on DEVICE-B to display the NTP configuration. ● DEVICE-B sends a time synchronization packet to 192.168.1.1 in order to synchronize time with DEVICE-A. ● After successfully synchronizing time with DEVICE-A, DEVICE-B can respond to the time synchronization request from DEVICE-C. ● Run the **show clock** command on DEVICE-B and DEVICE-C to check whether the time synchronization is successful.

Local Clock Reference Mode of NTP

Scenario Figure 5-6	
	● DEVICE-B configures the local clock as the NTP reference clock source. ● DEVICE-C synchronizes time with DEVICE-B.
Configuration Steps	● DEVICE-B configures the local clock as the NTP reference clock source. ● DEVICE-C configures DEVICE-B as the reference clock source.
DEVICE-B	B#configure terminal B(config)# ntp master B(config)# exit
DEVICE-C	C#configure terminal C(config)# ntp server 192.168.2.1 C(config)# exit
Verification	● Run the **show clock** command on DEVICE-C to check whether the time synchronization is successful.

6.4.2 Configuring NTP Security Authentication

Configuration Effect

Synchronizing Time from a Trusted Reference Clock Source

Use a device as a client to synchronize time only from a trusted external reference clock source to the local clock.

Providing Time Synchronization for a Trusted Device

Use the local clock of a device as the NTP reference clock source to provide time synchronization for only a trusted device.

Notes

The authentication keys of the client and server must be the same.

Configuration Steps

Configuring a Global Security Authentication Mechanism for NTP

- Mandatory.
- By default, a device disables the security authentication mechanism.

Configuring a Global Authentication Key for NTP

- Mandatory.
- By default, a device is not configured with an authentication key.

Configuring a Globally Trusted Key ID for NTP

- Optional.
- To provide time synchronization for a trusted device, you must specify a trusted authentication key by using the key ID.
- Only one trusted key can be configured. The specified authentication key must be consistent with that of the trusted device.

Configuring an Authentication Key ID for an External Reference Clock Source

- Optional.
- To synchronize time with a trusted reference clock source, you must specify a trusted authentication key by using the key ID.
- Each trusted reference clock source is mapped to an authentication key. The authentication keys must be consistent with the keys of trusted reference clock sources.

Verification

- Run the **show run** command to verify the NTP configuration.
- Run the **show clock** command to check whether time is synchronized only with a trusted device.

Related Commands

Enabling a Security Authentication Mechanism

Command	ntp authenticate
Parameter Description	N/A
Command	Global configuration mode

Mode	
Usage Guide	By default, a client does not use a global security authentication mechanism. If no security authentication mechanism is used, communication will not be encrypted. A global security indicator is not enough to imply that the communication between the client and server is implemented in an encrypted manner. Other global keys and an encryption key for the server must also be configured for initiating encrypted communication between the client and server.

Configuring a Global Authentication Key

Command	**ntp authentication-key** *key-id* **md5** *key-string* [*enc-type*]
Parameter Description	*key-id*: indicates the ID of a global authentication key, ranging from 1 to 4294967295. *key-string*: indicates a key string. *enc-type*: (optional) indicates whether an entered key is encrypted. 0 indicates no encryption, and 7 indicates simple encryption. The default setting is no encryption.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring a Trusted Key for NTP

Command	**ntp trusted-key** *key-id*
Parameter Description	*key-id*: Indicates the ID of a trusted key, ranging from 1 to 4294967295.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring a Trusted Key for an External Reference Clock Source

Refer to the section "Related Commands".

Configuration Example

Security Authentication

Scenario Figure 5-7	
	● DEVICE-B is configured to the NTP client/server mode and provides NTP services requiring security authentication for DEVICE-C. The authentication key is "abcd". ● DEVICE-A is used as the reference clock source of DEVICE-B. ● DEVICE-C synchronizes time with DEVICE-B.

Configuration Steps	● DEVICE-B configures DEVICE-A as the reference clock source. ● DEVICE-C configures DEVICE-B as the reference clock source.
DEVICE-B	B#configure terminal B(config)# ntp authentication-key 1 md5 abcd B(config)# ntp trusted-key 1 B(config)# ntp server 192.168.1.1 B(config)# exit
DEVICE-C	C#configure terminal C(config)# ntp authentication-key 1 md5 abcd C(config)# ntp server 192.168.2.1 key 1 C(config)# exit
Verification	● DEVICE-B sends a time synchronization packet that carries authentication information to 192.168.1.1 in order to synchronize time with DEVICE-A. ● Run the **show clock** command on DEVICE-B to check whether the time synchronization is successful.

6.4.3 Configuring NTP Access Control

Configuration Effect

Access control for NTP services provides a minimum security measure. A more secure method is to use an NTP authentication mechanism.

Notes

- Currently, the system does not support control query (used to control NTP servers by using network management devices, such as setting the leap second indicator or monitoring its working status). Though rule matching is implemented in the preceding sequence, no request related to control query is supported.
- If no access control rule is configured, all accesses are allowed. If any access control rule is configured, only accesses allowed by the rule can be implemented.

Related Configuration

Configuring the Access Control Rights for NTP

- Optional.
- Run the **ntp access-group** command to configure the access control rights and a corresponding ACL for NTP.

Verification

Run the show run command to verify the NTP configuration.

Related Commands

Configuring the Access Control Rights for NTP Services

Command	**ntp access-group** { **peer** | **serve** |**serve-only** | **query-only** }*access-list-number* | *access-list-name*
Parameter Description	**peer**: allows time request and control query for local NTP services, and allows a local device to synchronize time with a remote system (full access rights). **serve**: allows time request and control query for local NTP services, but does not allow a local device to synchronize time with a remote system. **serve-only**: allows only time request for local NTP services. **query-only**: allows only control query for local NTP services. *access-list-number*: indicates the number of an IP ACL, ranging from 1 to 99 and from 1300 to 1999. For details about how to create an IP ACL, refer to the *Configuring ACL*. *access-list-name*: indicates the name of an IP ACL. For details about how to create an IP ACL, refer to the *Configuring ACL*.
Command Mode	Global configuration mode
Usage Guide	Configure NTP access control rights. When an access request arrives, the NTP service matches rules in the sequence from the minimum access restriction to the maximum access restriction and uses the first matched rule. The matching sequence is peer, serve, serve-only, and query-only.

Configuration Example

Configuring NTP Access Control Rights

Configuration Steps	Allow only the device with the IP address of 192.168.1.1 to send a time synchronization request to a local device.
	FS(config)# access-list 1 permit 192.168.1.1 FS(config)# ntp access-group serve-only 1

6.5 Monitoring

Displaying

Description	Command
show ntp status	Displays the current NTP information.

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
debug ntp	Enables debugging.
no debug ntp	Disables debugging.

7 Configuring SNTP

7.1 Overview

The Simple Network Time Protocol (SNTP) is a simplified version of Network Time Protocol (NTP), which is used to synchronize the clocks of computers on the Internet. SNTP is applied in scenarios where it is unnecessary to use all NTP functions.

NTP uses a complex algorithm and has higher requirements for the system whereas SNTP uses a simpler algorithm and provides higher performance. Generally, SNTP precision can reach about 1s, which meets the basic requirements of most scenarios. Since SNTP packets are the same as NTP packets, the SNTP client implemented on a device is fully compatible with an NTP server.

Protocols and Standards

- RFC 2030: Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI

7.2 Applications

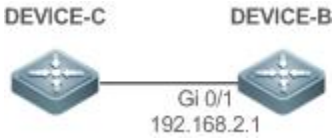
Application	Description
Synchronizing Time with an NTP Server	A device is used as a client to synchronize time with an NTP server.

7.2.1 Synchronizing Time with an NTP Server

Scenario

As shown in Figure 6-1, DEVICE-B uses a local clock as the NTP clock reference source and provides time synchronization for DEVICE-C. DEVICE-C is used as an SNTP client to synchronize time with DEVICE-B.

Figure 6-1



Deployment

- Specify DEVICE-B as the SNTP server of DEVICE-C.
- Enable SNTP for DEVICE-C.

7.3 Features

Basic Concepts

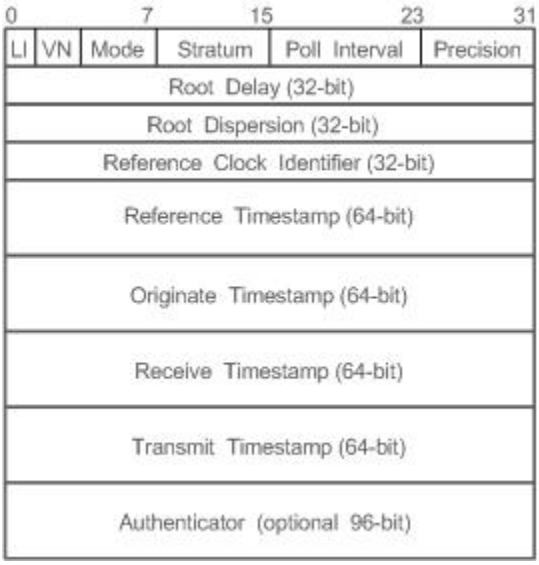
↘ SNTP Packet

SNTPV4 is developed from NTP, which is intended to simplify the functions of NTP. It does not change the NTP specifications and the original implementation of NTP. The message format of SNTPV4 is the same as that of NTP defined in RFC1305, with only some data fields initialized into preset values.

As defined in RFC1305, SNTP uses User Datagram Protocol (UDP) packets for transmission and the used UDP port ID is 123.

Figure 6-2 shows the format of an SNTP time synchronization packet.

Figure 6-2 Format of an SNTP Time Synchronization Packet



- Leap Indicator(LI): indicates a 2-bit leap second indicator.

00: indicates no warning information; 01: indicates that there are 61 seconds in the previous minute; 10: indicates that there are 59 seconds in the previous minute; 11: indicates that the clock is not synchronized.

- Version Number(VN): indicates a 3-bit NTP/SNTP version number. The current version number is 3.
- Mode: indicates a 3-bit SNTP/NTP working mode.

0: indicates no definition; 1: indicates symmetric active; 2: indicates symmetric passive; 3: indicates a client; 4: indicates a server; 5: indicates broadcasting; 6: indicates control information; 7: reserved.

- Stratum: indicates the 8-bit stratum of a local clock. 0: indicates no definition; 1: indicates the master clock reference source; other values: indicate slave clock reference sources.
- Poll Interval: indicates the poll interval (seconds), which is a 8-bit integer.
- Precision: indicates the time precision (seconds) of a local clock, which is a 8-bit integer.
- Root Delay: indicates the round-trip time to the master clock reference source, which is a 32-bit integer.
- Root Dispersion: indicates the largest difference from the master reference clock source, which is a 32-bit integer.
- Reference Clock Identifier: indicates the 32-bit identifier of a reference clock source.
- Reference Timestamp: indicates a 64-bit timestamp, namely, the time that is set or corrected at the last time.
- Originate Timestamp: indicates a 64-bit timestamp, namely, the local time when a time synchronization request leaves from a client.
- Receive Timestamp: indicates a 64-bit timestamp, namely, the local time when a time synchronization request packet arrives at a server.
- Transmit Timestamp: indicates a 64-bit timestamp, namely, the local time when a time synchronization response packet leaves from a server.
- Authenticator (optional): indicates authentication information.

Overview

Feature	Description
SNTP Time Synchronization	Synchronizes time from an SNTP/NTP server to a local device.

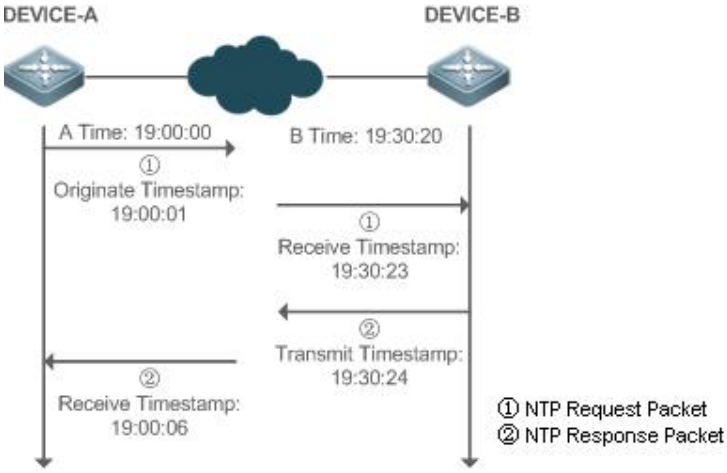
7.3.1 SNTP Time Synchronization

Working Principle

SNTP time synchronization is implemented by interaction of SNTP/NTP packets between a client and a server. The client sends a time synchronization packet to the server at intervals (half an hour by default). After receiving a response packet from the server, the client synchronizes time.

Figure 6-3 shows the format of an SNTP time synchronization packet.

Figure 6-3 Working Principle of SNTP



DEVICE-B (B for short) is used as an NTP reference clock source, DEVICE-A (A for short) is used as an SNTP client that synchronizes time with DEVICE-B. At a time point, the local clock of A is 19:00:00 and the local clock of B is 19:30:20.

12. A sends an SNTP/NTP request packet. The local time (T0) when the packet leaves from A is 19:00:00 and is filled in Originate Timestamp.
13. After a 2-second network delay, the local time (T1) when B receives the request packet is 19:30:23 and is filled in Receive Timestamp.
14. B processes the NTP request and sends an NTP response packet one second later. The local time (T2) when the response packet leaves from B is 19:30:24 and is filled in Transmit Timestamp.
15. After a 2-second network delay, A receives the response packet. The local time (T3) when the response packet arrives at A is 19:00:06.

The specific calculations for time synchronization are as follows:

- A obtains the time difference of 30 minutes and 20 seconds between B and A by using the formula ((T1-T0)+(T2-T3))/2.
- A obtains the packet round-trip delay of four seconds between A and B by using the formula (T3-T0)-(T2-T1).

Related Configuration

Enabling SNTP

- SNTP is disabled by default.
- Run the **sntp enable** command to enable SNTP.

Configuring an SNTP Server

- By default, no SNTP server is configured.
- Run the **sntp server** command to specify an SNTP server.

Configuring the SNTP Time Synchronization Interval

- By default, the SNTP time synchronization interval is 1,800s.
- Run the **sntp interval** command to specify the time synchronization interval.

7.4 Configuration

Configuration	Description and Command	
Configuring SNTP	(Mandatory) It is used to enable SNTP.	
	sntp enable	Enables SNTP.
	sntp server	Configures the IP address of an SNTP server.
	(Optional) It is used to configure the SNTP time synchronization interval.	
	sntp interval	Configures the SNTP time synchronization interval.

7.4.1 Configuring SNTP

Configuration Effect

An SNTP client accesses an NTP server at fixed intervals to correct the clock regularly.

Notes

All time obtained through SNTP communication is Greenwich Mean Time (GMT). To obtain precise local time, you need to set the local time zone for alignment with GMT.

Configuration Steps

Enabling SNTP

- (Mandatory) SNTP is disabled by default.

Configuring the IP address of an SNTP Server

- (Mandatory) No SNTP/NTP server is configured by default.

Configuring the SNTP Time Synchronization Interval

- Optional.

- By default, a device synchronizes time every half an hour.

Verification

Run the show sntp command to display SNTP-related parameters.

Related Commands

Enabling SNTP

Command	**sntp enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	SNTP is disabled by default. Run the **no sntp enable** global configuration command to disable SNTP.

Configuring the IP address of an SNTP/NTP Server

Command	**sntp server** [**oob**] { *ip- address* / *domain* } [**source** *source-ip-address*]
Parameter Description	*ip-address*: indicates the IP address of an SNTP server. No SNTP server is configured by default. *domain:* domain name of the SNTP server. No SNTP server is configured by default. **oob**: Indicates that the SNTP server supports an out-band management interface. *source-ip-address:* Indicates the source IP address.
Command Mode	Global configuration mode
Usage Guide	Since SNTP is fully compatible with NTP, the server can be configured as a public NTP server on the Internet. Since SNTP packets are the same as NTP packets, the SNTP client is fully compatible with the NTP server. There are many NTP servers on the Internet. You can select an NTP server with a shorter delay as the SNTP server on your device.

Configuring the SNTP Time Synchronization Interval

Command	**sntp interval** *seconds*
Parameter Description	*seconds*: Indicates the time synchronization interval, ranging from 60s to 65,535s. The default value is 1,800s.
Command Mode	Global configuration mode
Usage Guide	Run this command to set the interval for an SNTP client to synchronize time with an NTP/SNTP server. The interval configured here does not take effect immediately. To make it take effect immediately, run the **sntp enable** command.

Configuration Example

SNTP Time Synchronization

Scenario Figure 6-4	
	● DEVICE-B indicates an NTP server on the Internet. ● DEVICE-C synchronizes time with DEVICE-B.
Configuration Steps	Enable SNTP for DEVICE-C and configure DEVICE-B as an NTP server.
DEVICE-C	C#configure terminal C(config)# sntp server 192.168.2.1 C(config)# sntp enable C(config)# exit
Verification	● Run the **show clock** command on DEVICE-C to check whether the time synchronization is successful. ● Run the **show sntp** command on DEVICE-C to display the SNTP status and check whether the server is successfully configured.

7.5 Monitoring

Displaying

Description	Command
show sntp	Displays SNTP-related parameters.

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
debug sntp	Enables debugging.

8 Configuring DNS Proxy

8.1 Overview

The DNS proxy, also referred to as forward DNS proxy, is deployed on the frontend egress gateway and located between a DNS server and user PC to resolve DNS requests on behalf of the DNS server.

The forward DNS proxy provides the following functions:

- Balancing load among multiple lines
- Any DNS
- DNS anti-hijacking

Protocol Specifications

- RFC1034: DOMAIN NAMES - CONCEPTS AND FACILITIES
- RFC1035: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

8.2 Applications

Application	Description
Balancing Load Among Mulitple Lines	If multiple ISP egress lines are deployed on an extranet, a DNS proxy can be configured on the egress gateway, so that the gateway can select ISP lines according to policies, thereby implementing load balancing among different lines.

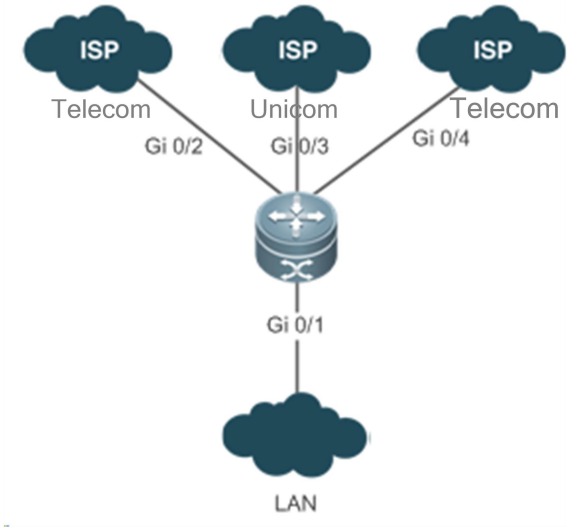
8.2.1 Balancing Load among Multiple Lines

Scenario

As shown in Figure 7-1, multiple ISP egress lines are deployed on an extranet: a Telecom egress line (1000 Mbps), a Unicom egress line (100 Mbps), and a Telecom PPP dial line (10 Mbps). The lines are respectively connected to the egress gateway through the interfaces Gi 0/2, Gi 0/3, and Gi 0/4. Telecom provides two DNS servers, and the active DNS server is at the IP address 218.85.157.99 and the standby DNS server is at the IP address 218.85.152.99. Unicom provides two DNS servers as well, and the active DNS server is at the IP address 58.22.96.66 and the standby DNS server is at the IP address 218.104.128.106.

Generally, only one fixed DNS server is enabled on an intranet client, which cannot realize the advantages of multiple egress interfaces and is likely to cause a great part of traffic to be born on one ISP line. Consequently, bandwidth of the selected ISP line is depleted while other lines are idle. If an ISP DNS server can be selected according to line load, line congestion and idling problems can be resolved.

Figure 7-1 DNS Line Topology



Deployment

- Enable the DNS proxy function on the interface Gi 0/1 of the egress gateway so that the DNS proxy can process DNS request packets received on this interface.
- Configure the Telecom DNS server on the interface Gi0/2 and the Unicom DNS server on the interface Gi0/3. No DNS server needs to be configured on the interface Gi 0/4, because the interface is connected to the PPP dial line of Telecom.

8.3 Features

Basic Concepts

DNS Resolution

Internet access is implemented based on an IP address. If a peer IP address is unknown, Internet access cannot be implemented. The DNS system is an IP address translation system that facilitates memorization. With a domain name, the DNS system can resolve the domain name and translate the domain name into an IP address. The DNS system is composed of a DNS server and a DNS client. The DNS server maintains a table of mapping between domain names and IP addresses. When the DNS client initiates a query request, the DNS server queries the table and sends the resolution result to the DNS client.

DNS Proxy

A DNS proxy is a proxy between the DNS server and DNS client. It can act as a DNS server to receive query requests from the DNS client. The DNS proxy can be visible or invisible to the DNS client. If the DNS proxy is configured as the default DNS server of the DNS client, the proxy is visible to the client. If the proxy intercepts packets sent from the client, the proxy is invisible to the client.

Overview

Feature	Description
Forward DNS Proxy	The DNS proxy processes query requests from a DNS client on behalf of the DNS server and supports functions such as balancing load among multiple lines, any DNS, and DNS anti-hijacking.

8.3.1 Forward DNS Proxy

Working Principle

When intercepting DNS packets, the DNS proxy selects a policy according to the functional module enabled to decide an egress interface, changes the destination IP address in the packets to the IP address of the DNS server configured on the egress interface, and then forwards the packets through the egress interface. The module is transparent to the intranet clients, and therefore the clients do not detect the DNS proxy.

The forward DNS proxy provides the following functions:

- **Balancing Load Among Multiple Lines**

To resolve northbound and southbound interconnection problems, multiple lines are deployed on the egress gateways of the networks in many enterprises and campuses, and technical means are used to separate Telecom access requests from Unicom access requests. Generally, only one fixed DNS server is enabled on an intranet client. As a result, most traffic is transmitted along one line, and other lines are idle.

The DNS proxy can select a DNS server according to the egress bandwidth or bandwidth utilization rate, enabling extranet access traffic to be balanced on different egress interfaces. By default, load balancing is implemented based on bandwidth. Greater bandwidth of a line indicates that the line is more possible to be selected. If load balancing is implemented based on bandwidth utilization rate, the line with the minimum egress traffic or bandwidth is selected.

Operators will provide a DNS server on each ISP line. When intercepting a DNS request packet, the DNS proxy selects an ISP line according to a policy and forwards the request packet to the DNS server corresponding to the line. If the destination IP address corresponds to the ISP line, the DNS response packet will carry the IP address, and subsequent traffic will be forwarded along this line, implementing load balancing between different lines. If the destination IP address does not correspond to the ISP line, the DNS response packet will carry an IP address of another ISP line, and subsequent traffic will be forwarded along this ISP line.

- **Any DNS**

The DNS proxy can determine whether a DNS server is properly set and automatically correct improper settings to ensure normal Internet access, regardless of the DNS server configuration. Improper settings include cross-operator access (for example, a Telecom user uses a DNS server of Unicom) and cross-area access (for example, a Telecom user from Fuzhou uses a DNS server in Beijing).

Upon receiving a request packet, the DNS proxy checks whether the source and destination IP addresses in the packet are proper and automatically corrects the improper destination IP address to a proper one. For a cross-operator access request, the access request will be changed to one operator; for a cross-area access request, the access request will be changed to the local area.

- **DNS Whitelist**

To prevent some DNS requests from being processed by the forward DNS proxy, users can add the matching rule of this type of packets to the DNS whitelist. In this case, the DNS proxy will not intercept or process the packets that match corresponding rules.

- **DNS Anti-hijacking**

The DNS proxy can avoid domain name hijacking if the client receives malicious DNS response packets. According to the DNS anti-hijacking blacklist configured by the administrator in advance, the DNS proxy checks whether the IP address corresponding to the domain name in a DNS response packet matches an IP address in the blacklist when forwarding the packet. If they match, the packet is discarded.

- **DNS Proxy and Route Association**

The forward DNS proxy is enabled for Telecom, Unicom, and the education network, and policy-based routing (PBR) is configured to force a part of traffic to be forwarded over the education network. In practice, the DNS proxy prevails over the PBR, and therefore the IP address resolved from a DNS packet by the DNS proxy may be different from that resolved by the DNS server on the education network. Besides, a part of traffic is forwarded over the education network according to the PBR. As a result, Internet access is affected due to cross-operator access. By association of the DNS proxy with a route, DNS packets and Internet access traffic are forwarded along different routes, and valid IP addresses can be obtained.

Related Configuration

Enabling Forward DNS Proxy on Egress Interfaces

- This function is disabled on the egress interfaces of the gateway by default.
- Run the **dns-proxy enable** command to enable this function.
- The DNS proxy can work properly only after this function is enabled.

Configuring Load Balancing

- The bandwidth-based policy is used by default.
- Run the **load-balance** {**load** | **bandwidth**} command to switch between load balancing based on bandwidth utilization rate and that based on bandwidth.

Configuring DNS Whitelist

- The DNS whitelist is empty by default.
- Run the **whitelist** {**source-ip** *start-ip* [*end-ip*] | **name-server** *ip* } [**increase** | **decrease** *num*] command to configure a DNS whitelist.

Configuring DNS Anti-hijacking

- The DNS anti-hijacking blacklist is empty by default.
- Run the **blacklist domain-ip** *start-ip* [*end-ip*] command to add IP addresses to a DNS anti-hijacking blacklist.

8.4 Configuration

Configuration	Description and Command	
Enabling Forward DNS Proxy	(Mandatory) It is used to create a DNS proxy.	
	dns-proxy enable	Enables the forward DNS proxy.
	ip name-server	Configures the DNS server for lines.
Configuring Load Balancing	Optional	
	load-balance	Switches between load balancing based on bandwidth and that based on bandwidth utilization rate.
Configuring DNS Whitelist	Optional	
	whitelist	Configures a DNS whitelist.

Configuring DNS Anti-hijacking	Optional	
	blacklist domain-ip	Add IP addresses to a DNS anti-hijacking blacklist.

8.4.1 Enabling Forward DNS Proxy

Configuration Effect

Enable the forward DNS proxy to select an egress line based on bandwidth and enable the any DNS function.

Notes

The DNS proxy must be configured on L3 interfaces.

Configuration Steps

Enabling Forward DNS Proxy

- Mandatory.
- Enable the DNS proxy on the LAN interface unless otherwise specified.

Configuring DNS Server for Lines

- Mandatory.
- Configure the DNS server on the WAN interfaces for lines unless otherwise specified.

Verification

- Run the show run or show dns-proxy configure command to display the DNS proxy configuration.

Related Commands

Enabling DNS Proxy

Command	**dns-proxy enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	The configured interface must be an L3 interface, for example, routing interface, L3AP, SVI, and loopback interface. All configured interfaces should be reachable through an IPv4 unicast route.

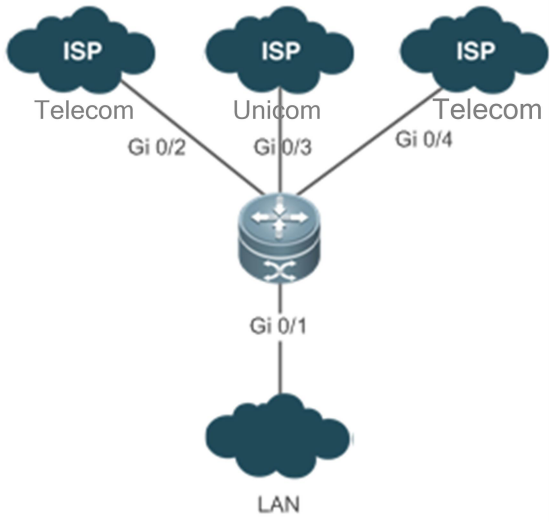
Configuring DNS Server for Lines

Command	**ip name-server** *ip-address* [**track** *id*]
Parameter Description	*ip-address*: Indicates the IP address of the DNS server. *id*: Indicates the ID of an associated track.

Command Mode	Interface configuration mode
Usage Guide	The DNS proxy can be used only after the DNS server is configured on a WAN interface. Generally, operators provide an active DNS server and a standby DNS server. Both the DNS servers can be configured on the WAN interface, so that the DNS proxy can enable the standby DNS server when the active one fails. A maximum of four DNS servers can be configured on one interface. Associate the DNS proxy with a track to check whether the link to the DNS server is reachable. If the association is not configured, the link is reachable when the interface is in the Up state.

Configuration Example

Enabling Forward DNS Proxy

Scenario Figure 7-2	As shown in Figure 7-2, multiple ISP egress lines are deployed on an extranet: a Telecom egress line, a Unicom egress line, and a Telecom PPP dial line. The lines are respectively connected to the egress gateway through the interfaces Gi 0/2, Gi 0/3, and Gi 0/4. The Telecom DNS server is configured at the IP address 218.85.157.99 and the Unicom DNS server is configured at the IP address 58.22.96.66.
	
Configuration Steps	● Enable the DNS proxy on the LAN interface connected to the intranet. ● Configure the DNS server on the WAN interfaces connected to the extranet.
	FS#configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#int gi0/1 FS(config-if-GigabitEthernet 0/1)#dns-proxy enable FS(config-if-GigabitEthernet 0/1)#exit FS(config)#int gi0/2 FS(config-if-GigabitEthernet 0/2)#ip name-server 218.85.157.99 track 1 FS(config-if-GigabitEthernet 0/2)#exit FS(config)#int gi0/3 FS(config-if-GigabitEthernet 0/3)#ip name-server 58.22.96.66 track 2

	FS(config-if-GigabitEthernet 0/3)#exit

Verification	● Check whether the DNS proxy is enabled.
	FS#show run | begin interface GigabitEthernet 0/1
	Current configuration : 491 bytes
	
	interface GigabitEthernet 0/1
	  dns-proxy enable
	!
	
	● Check whether the DNS server is configured for lines.
	FS#show run | begin interface GigabitEthernet 0/2
	Current configuration : 491 bytes
	
	interface GigabitEthernet 0/2
	  ip name-server 218.85.157.99 track 1
	!
	interface GigabitEthernet 0/3
	  ip name-server 58.22.96.66 track 2
	!

8.4.2 Configuring Load Balancing

Configuration Effect

Implement load balancing based on bandwidth by default. Greater bandwidth of a line indicates that the line is more possible to be selected.
Select the line with the minimum egress traffic or bandwidth if load balancing is implemented based on bandwidth utilization rate.

Configuration Steps

Switching Between Load Balancing Based on Bandwidth and That Based on Bandwidth Utilization Rate

- Optional.
- Implement load balancing based on bandwidth by default. Users can switch from load balancing based on bandwidth to that based on bandwidth utilization rate.

Verification

- Run the **show run** or **show dns-proxy configure** command to display the DNS proxy configuration.

Related Commands

Switching Between Load Balancing Based on Bandwidth and That Based on Bandwidth Utilization Rate

Command	**load-balance {load | *bandwidth*}**
Parameter Description	**load**: Indicates the bandwidth-based policy. *bandwidth*: Indicates the bandwidth utilization rate-based policy.
Command Mode	DNS proxy mode
Usage Guide	By default, load balancing is implemented based on bandwidth. Users can enter the DNS proxy mode and manually switch from load balancing based on bandwidth to that based on bandwidth utilization rate.

Configuration Example

Changing Load Balancing Policy

Scenario	For details, refer to Figure 7-2.
Configuration Steps	Configure bandwidth utilization rate-based load balancing for the DNS proxy.
	FS#configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#dns-proxy FS(config-dns-proxy)#load-balance load

Verification	● Check whether the DNS proxy is enabled.
	FS#show run | begin interface GigabitEthernet 0/1
	Current configuration : 491 bytes
	
	interface GigabitEthernet 0/1
	  dns-proxy enable
	!
	
	● Check whether load balancing that is based on bandwidth utilization rate is configured for the DNS proxy.
	FS#show run | begin dns-proxy
	Current configuration : 491 bytes
	
	dns-proxy
	  load-balance load
	!

8.4.3 Configuring DNS Whitelist

Configuration Effect

Enable users to add a network segment or domain names into a DNS whitelist. DNS request packets with IP addresses or domain names matching the DNS whitelist will not be intercepted directly by the DNS proxy.

Configuration Steps

Configuring DNS Whitelist

- Optional.

Verification

- Run the **show run** or **show dns-proxy configure** command to display the DNS proxy configuration.

Related Commands

Configuring DNS Whitelist

Command	**whitelist** {**source-ip** *start-ip* [*end-ip*] | **name-server** *ip* } [**increase** | **decrease** *num*]
Parameter Description	*start-ip*: Indicates a start IP address. *end-ip*: Indicates an end IP address. *ip*: Indicates the IP address of a DNS server. *num*: Indicates a priority. The priority configured later is higher than that configured earlier. Increase or decrease the row number to change the priority.
Command Mode	DNS proxy mode
Usage Guide	Enable users to add a network segment or domain names into a DNS whitelist. DNS request packets with IP addresses or domain names matching the DNS whitelist will not be intercepted directly by the DNS proxy.

Configuration Example

Configuring DNS Whitelist

Scenario	For details, refer to Figure 7-2.
Configuration Steps	Enable the DNS whitelist function. 1. Configure a whitelist that is based on the source IP addresses in the network segment 192.168.1.1–192.168.1.10. 2. Configure a whitelist that is based on IP addresses of DNS servers. 3. Configure a whitelist that is based on domain names.
	FS#configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#dns-proxy FS(config-dns-proxy)#dns-proxy whitelist source-ip 192.168.1.1 192.168.1.10 FS(config-dns-proxy)#dns-proxy whitelist name-server 8.8.8.8
Verification	● Check whether the DNS proxy is enabled. FS#show run | begin interface GigabitEthernet 0/1 Current configuration : 491 bytes

```
interface GigabitEthernet 0/1
 dns-proxy enable!
```

- Check whether a DNS whitelist is configured.

```
FS#show run | begin dns-proxy
Current configuration : 491 bytes

dns-proxy
 dns-proxy whitelist source-ip 192.168.1.1 192.168.1.10
 dns-proxy whitelist name-server 8.8.8.8
!
```

8.4.4 Configuring DNS Anti-hijacking

Configuration Effect

Enable the DNS proxy to determine whether the destination IP address in a DNS response packet comes from a malicious site according to a blacklist. If yes, the DNS proxy filters out the packet to protect the client from being hijacked during normal Internet access.

Configuration Steps

Configuring DNS Anti-hijacking Blacklist

- Mandatory.

Verification

- Run the **show run** or **show dns-proxy configure** command to display the DNS proxy configuration.

Related Commands

Configuring DNS Anti-hijacking Blacklist

Command	**blacklist domain-ip** *start-ip [end-ip]*
Parameter Description	*start-ip*: Indicates a start IP address. *end-ip*: Indicates an end IP address.
Command Mode	DNS proxy mode
Usage Guide	Some Internet malicious programs may masquerade as a DNS server to send DNS response packets, directing clients to access an invalid IP address. The procedure is referred to as DNS hijacking. A DNS blacklist contains such invalid IP addresses. With the blacklist, the DNS proxy discards packets that direct clients to such IP addresses.

Configuration Example

Configuring DNS Anti-hijacking

Scenario	For details, refer to Figure 7-2.
Configuration Steps	Configure a blacklist containing the destination IP address segment 202.112.14.1–202.114.14.10 for the DNS proxy.
	FS#configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#dns proxy FS(config-dns-proxy)# blacklist domain-ip 202.112.14.1 202.114.14.10
Verification	Check whether a DNS anti-hijacking blacklist is configured. FS#show run | begin dns-proxy Current configuration : 491 bytes dns-proxy blacklist domain-ip 202.112.14.1 202.114.14.10 !

8.5 Monitoring

Clearing

Description	Command
Clears the statistical information of the DNS proxy.	**clear dns-proxy statistics**

Displaying

Description	Command
Displays the DNS proxy configuration.	**show dns-proxy configure**
Displays the whitelist configuration of the DNS proxy.	**show dns-proxy configure whitelist**
Displays the anti-hijacking configuration of the DNS proxy.	**show dns-proxy configure blacklist**
Displays the DNS server configuration of the DNS proxy.	**show dns-proxy name-server**
Displays the statistical information of the DNS proxy.	**show dns-proxy statistics**

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command

Debugs the DNS proxy switch.	**debug dns-proxy**

9 Configuring FTP Server

9.1 Overview

The File Transfer Protocol (FTP) server function enables a device to serve as an FTP server. In this way, a user can connect an FTP client to the FTP server and upload files to and download files from the FTP server through FTP.

A user can use the FTP server function to easily obtain files such as syslog files from a device and copy files to the file system of the device through FTP.

Protocols and Standards

- RFC959: FILE TRANSFER PROTOCOL (FTP)
- RFC3659: Extensions to FTP
- RFC2228: FTP Security Extensions
- RFC1635: How to Use Anonymous FTP

9.2 Applications

Application	Description
Providing FTP Services in a LAN	Provides the uploading and downloading services for a user in a Local Area Network (LAN).

9.2.1 Providing FTP Services in a LAN

Scenario

Provide the uploading and downloading services for a user in a LAN.

As shown in Figure 8-1, enable the FTP server function only in a LAN.

- G and S are enabled with the FTP server function and layer-2 transparent transmission function respectively.
- A user initiates a request for FTP uploading and downloading services.

Figure 8-1

Remarks	G is an egress gateway device. S is an access device.

Deployment

- G is enabled with the FTP server function.
- As a layer-2 switch, S provides the function of layer-2 transparent transmission.

9.3 Features

Basic Concepts

FTP

FTP is a standard protocol defined by the IETF Network Working Group. It implements file transfer based on the Transmission Control Protocol (TCP). FTP enables a user to transfer files between two networked computers and is the most important approach to transferring files on the Internet. A user can obtain abundant Internet for free through anonymous FTP. In addition, FTP provides functions such as login, directory query, file operation, and other session control. Among the TCP/IP protocol family, FTP is an application-layer protocol and uses TCP ports 20 and 21 for transmission. Port 20 is used to transmit data and port 21 is used to transmit control messages. Basic operations of FTP are described in RFC959.

User Authorization

To connect an FTP client to an FTP server, you should have an account authorized by the FTP server. That is, a user can enjoy services provided by the FTP server after logging in to the FTP server with a user name and password. A maximum of 10 accounts can be configured, a maximum of 2 connections are allowed for each account, and a maximum of 10 connections are supported by the server.

FTP File Transmission Modes

FTP provides two file transmission modes:

- Text transmission mode (ASCII mode): It is used to transfer text files (such as .txt, .bat, and .cfg files). This mode is different from the binary mode in carriage return and line feed processing. In ASCII mode, carriage return and line feed are changed to local CRC characters, for example, \n in Unix, \r\n in Windows, and \r in Mac. Assume that a file being copied contains ASCII text. If a remote computer does not run Unix, FTP automatically converts the file format to suit the remote computer.
- Binary transmission mode: It is used to transfer program files (for example, .app, .bin and .btm files), including executable files, compressed files and image files without processing data. Therefore, Binary mode facilitates faster transfer of all files and more reliable transfer of ASCII files.

FTP Working Modes

FTP provides two working modes:

Figure 8-2

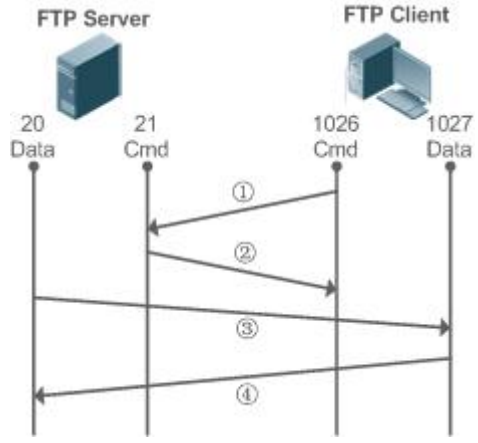
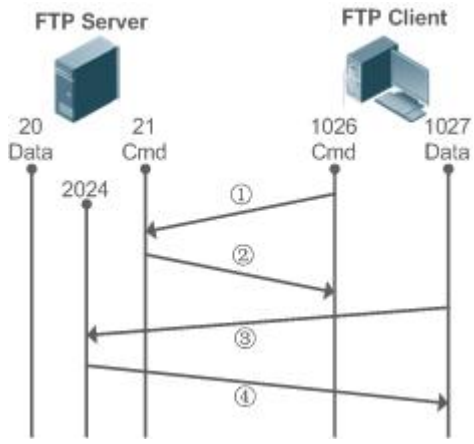


Figure 8-3



- Figure 8-2 shows the active (PORT) mode. The FTP client uses port 1026 to connect to the FTP server through port 21. The client sends commands through this channel. Before receiving data, the client sends the **PORT** command on this channel. The **PORT** command contains information on the channel port (1027) of the client for receiving data. The server uses port 20 to connect to the client through port 1027 for establishing a data channel to receive and transmit data. The FTP server must establish a new connection with the client for data transmission.
- passive (PASV) mode. The process for establishing a control channel is similar to that in the PORT mode. However, after the connection is established, the client sends the **PASV** command rather than the **PORT** command. After receiving the **PASV** command, the FTP server enables a high-end port (2024) at random and notifies the client that data will be transmitted on this port. The client uses port 1027 to connect the FTP server through port 2024. Then, the client and server can transmit and receive data on this channel. In this case, the FTP server does not need to establish a new connection with the client.

Supported FTP Commands

After receiving an FTP connection request, the FTP server requires the client to provide the user name and password for authentication.
If the client passes the authentication, the FTP client commands can be executed for operations. The available FTP client commands are listed as follows:

ascii	delete	mdelete	mput	quit	send
bin	dir	mdir	nlist	recv	size
bye		mget		rename	system
cd	get	mkdir	passive		type
cdup		mls	put	rmdir	user
close	ls		pwd		

For usage of these FTP client commands, please refer to your FTP client software document. In addition, many FTP client tools (such as CuteFTP and FlashFXP) provide the graphic user interface. These tools facilitate operations by freeing users from configuring FTP commands.

Overview

Feature	Description
Enabling the FTP Server Function	Provides the functions of uploading, downloading, displaying, creating and deleting files for an FTP client.

9.3.1 Enabling the FTP Server Function

Working Principle

The basic working principle is described in the previous chapter. FS devices provide FTP services after the user name, password, and top-level directory are configured.

Related Configuration

Enabling the FTP Server Function Globally

The FTP server function is disabled by default.

Run the ftp-server enable command to enable the FTP server function.

You must enable the FTP server function globally before using it.

Configuring a User Name, Password, and Top-Level Directory

There is no authorized user or top-level directory by default.

Run the ftp-server username password and ftp-server topdir commands to set an authorized user and top-level directory.

The three configurations above are mandatory; otherwise, the FTP server function cannot be enabled.

9.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions	(Mandatory) It is used to enable an FTP server.	
	ftp-server enable	Enables the FTP server function.
	ftp-server login timeout	Configures Login timeout for an FTP session.
	ftp-server login times	Configures the valid login count.
	ftp-server topdir	Configures the top-level directory of the FTP server.
	ftp-server username password	Configures a user name and password.
	Optional.	
	ftp-server timeout	Configures the idle timeout of an FTP session.

9.4.1 Configuring Basic Functions

Configuration Effect

- Create an FTP server to provide FTP services for an FTP client.

Notes

- The user name, password, and top-level directory need to be configured.
- To enable the server to close an abnormal session within a limited period, you need to configure the idle timeout of a session.

Configuration Steps

Enabling the FTP Server Function

- Mandatory.
- Unless otherwise noted, enable the FTP server function on every router.

Configuring a Top-Level Directory

- Mandatory.
- Unless otherwise noted, configure the top-level directory as the root directory on every router.

Configuring a User Name and Password for Login

- Mandatory.
- The lengths of the user name and password are restricted.

Configuring the Login Timeout for an FTP Session

- Optional.
- When the client is disconnected from the server due to an error or other abnormal causes, the FTP server may not know that the user is disconnected and continues to keep the connection. Consequently, the FTP connection is occupied for a long time and the server cannot respond to the login requests of other users. This configuration can ensure that other users can connect to the FTP server within a period of time upon an error.

Verification

Connect an FTP client to the FTP server.

- Check whether the client is connected.
- Check whether operations on the client are normal.

Related Commands

Enabling the FTP Server Function

Command	**ftp-server enable**
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	The client cannot access the FTP server unless the top-level directory, user name and password are configured. Therefore, it is recommended that you configure the top-level directory, user name and password for login by referring to the subsequent chapters before enabling the service for the first time.

Configuring the Valid Login Count

Command	**ftp-server login times** *times*

Parameter Description	*times:* Indicates the valid login count, ranging from 1 to 10.
Command Mode	Global configuration mode
Usage Guide	The valid login count refers to the number of times you can perform account verification during an FTP session. The default value is 3, which means that your session will be terminated if you enter an incorrect user name or password for three times and other users can go online.

Configuring the Login Timeout for an FTP Session

Command	**ftp-server login timeout** *timeout*
Parameter Description	*timeout*: Indicates the login timeout, ranging from 1 to 30 minutes.
Command Mode	Global configuration mode
Usage Guide	The login timeout refers to the maximum duration that the session lasts since being established. If you do not pass the password verification again during the login timeout, the session will be terminated to ensure that other users can log in.

Configuring the Top-Level Directory of the FTP Server

Command	**ftp-server topdir** *directory*
Parameter Description	*directory:* Indicates the user access path.
Command Mode	Global configuration mode
Usage Guide	If the top-level directory of the server is set to "/syslog", the FTP client can access only the files and directories in the "/syslog" directory on the device after login. Due to restriction on the top-level directory, the client cannot return to the upper directory of "/syslog".

Configuring a User Name and Password for Server Login

Command	**ftp-server username** *username* **password** [*type*] *password*
Parameter Description	***Username***: Indicates a user name. *type*: 0 or 7. 0 indicates that the password is not encrypted (plaintext) and 7 indicates that the password is encrypted (cipher text). **password**: Indicates a password.
Command	Global configuration mode

Mode	
Usage Guide	The FTP server does not support anonymous login; therefore, a user name must be configured. A user name consists of up to 64 characters including letters, half-width digits and symbols without spaces. A password consists of only letters or digits. Spaces at the beginning and end of the password are ignored. Spaces inside the password are viewed as part of the password. A plaintext password consists of 1 to 25 characters. A cipher text password consists of 4 to 52 characters. User names and passwords must match. A maximum of 10 users can be configured.

Configuring the Idle Timeout for an FTP Session

Command	**ftp-Server timeout** *time*
Parameter Description	*time*: Indicates the idle timeout, ranging from 1 to 3,600 minutes.
Command Mode	Global configuration mode
Usage Guide	The idle timeout of a session refers to the duration from the end of an FTP operation to the start of the next FTP operation in an FTP session. After the server responds to an FTP client command operation (for example, after a file is completely transferred), the server starts to count the idle time again, and stops when the next FTP client command operation arrives. Therefore, the configuration of the idle timeout has no effect on some time-consuming file transfer operations.

Displaying Server Status

Command	**show ftp-server**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Run this command to display FTP server status.

Debugging

Command	**debug ftp-server pro/err**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Run this command to debug message/error events of the FTP server.

Configuration Example

Creating an FTP Server on an IPv4 Network

Scenario	● A TCP connection is established for transmission from a server to a client.
Configuration Steps	● Enable the FTP server function. ● Configure the top-level directory/syslog. ● Set the user name **user** and password to **password**. ● Set the session idle timeout to 5 minutes.
	FS(config)#ftp-server username user FS(config)#ftp-server password password FS(config)#ftp-server timeout 5 FS(config)#ftp-server topdir / FS(config)#ftp-server enable
Verification	Run the **show ftp-server** command to check whether the configuration takes effect.
	FS#show ftp-server ftp-server information ========== enable : Y topdir : tmp:/ timeout: 10min username:aaaa password:(PLAINT)bbbb connect num[2] [0]trans-type:BINARY (ctrl)server IP:192.168.21.100[21] client IP:192.168.21.26[3927] [1]trans-type:ASCII (ctrl)server IP:192.168.21.100[21] client IP:192.168.21.26[3929] username:a1 password:(PLAINT)bbbb connect num[0] username:a2 password:(PLAINT)bbbb connect num[0] username:a3 password:(PLAINT)bbbb connect num[0] username:a4 password:(PLAINT)bbbb connect num[0] username:a5 password:(PLAINT)bbbb connect num[0] username:a6 password:(PLAINT)bbbb connect num[0] username:a7 password:(PLAINT)bbbb connect num[0] username:a8 password:(PLAINT)bbbb connect num[0] username:a9 password:(PLAINT)bbbb connect num[0]

Common Errors

- No user name is configured.
- No password is configured.
- No top-level directory is configured.

9.5 Monitoring

Displaying

Description	Command
Displays the FTP server configuration.	show ftp-server

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the FTP server error events.	**debug ftp-server err**
Debugs the FTP server message events.	**debug ftp-server pro**

10 Configuring Time Range

10.1 Overview

Time Range is a time-based control service that provides some applications with time control. For example, you can configure a time range and associate it with an access control list (ACL) so that the ACL takes effect within certain time periods of a week.

10.2 Typical Application

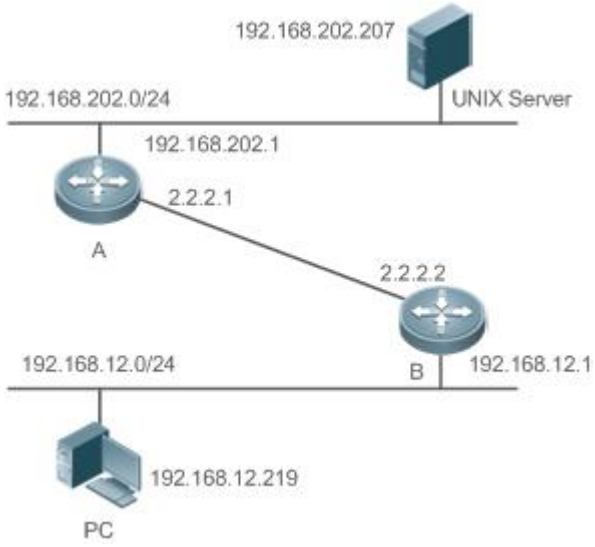
Typical Application	Scenario
Applying Time Range to an ACL	Apply a time range to an ACL module so that the time-based ACL takes effect.

10.2.1 Applying Time Range to an ACL

Application Scenario

An organization allows users to access the Telnet service on a remote Unix host during working hours only, as shown in Figure 9-1.

Figure 9-1



Note	Configure an ACL on device B to implement the following security function: Hosts in network segment 192.168.12.0/24 can access the Telnet service on a remote Unix host during normal working hours only.

Functional Deployment

- On device B, apply an ACL to control Telnet service access of users in network segment 192.168.12.0/24. Associate the ACL with a time range, so that the users' access to the Unix host is allowed only during working hours.

10.3 Function Details

Basic Concepts

Absolute Time Range

The absolute time range is a time period between a start time and an end time. For example, [12:00 January 1 2000, 12:00 January 1 2001] is a typical absolute time range. When an application based on a time range is associated with the time range, a certain function can be effective within this time range.

Periodic Time

Periodic time refers to a periodical interval in the time range. For example, "from 8:00 every Monday to 17:00 every Friday" is a typical periodic time interval. When a time-based application is associated with the time range, a certain function can be effective periodically from every Monday to Friday.

Features

Feature	Function
Using Absolute Time Range	Sets an absolute time range for a time-based application, so that a certain function takes effect within the absolute time range.
Using Periodic Time	Sets periodic time or a time-based application, so that a certain function takes effect within the periodic time.

10.3.1 Using Absolute Time Range

Working Principle

When a time-based application enables a certain function, it determines whether current time is within the absolute time range. If yes, the function is effective or ineffective at the current time depending on specific configuration.

Related Configuration

Configuring Time Range

No time range is configured by default.
Use the time-range time-range-name command to configure a time range.

Configuring Absolute Time Range

The absolute time range is [00:00 January 1, 0, 23:59 December 31, 9999] by default.
Use the absolute { [start time date] | [end time date] } command to configure the absolute time range.

10.3.2 Using Periodic Time

Working Principle

When a time-based application enables a certain function, it determines whether current time is within the period time. If yes, the function is effective or ineffective at the current time depending on specific configuration.

Related Configuration

Configuring Time Range

No time range is configured by default.
Use the time-range time-range-name command to configure a time range.

Configure Periodic Time

No periodic time is configured by default.

Use the periodic day-of-the-week time to [day-of-the-week] time command to configure periodic time.

10.4 Configuration Details

Configuration Item	Suggestions and Related Commands	
Configuring Time Range	Mandatory configuration. Time range configuration is required so as to use the time range function.	
	time-range *time-range-name*	Configures a time range.
	Optional configuration. You can configure various parameters as necessary.	
	absolute { [**start** *time date*] | [**end** *time date*] }	Configures an absolute time range.
	periodic *day-of-the-week time* **to** [*day-of-the-week*] *time*	Configures periodic time.

10.4.1 Configuring Time Range

Configuration Effect

- Configure a time range, which may be an absolute time range or a periodic time interval, so that a time-range-based application can enable a certain function within the time range.

Configuration Method

Configuring Time Range

- Mandatory configuration.
- Perform the configuration on a device to which a time range applies.

Configuring Absolute Time Range

- Optional configuration.

Configuring Periodic Time

- Optional configuration.

Verification

- Use the **show time-range** [*time-range-name*] command to check time range configuration information.

Related Commands

Configuring Time Range

Command	**time-range** *time-range-name*

Parameter Description	*time-range-name*: name of the time range to be created.
Command Mode	Global configuration mode
Usage Guide	Some applications (such as ACL) may run based on time. For example, an ACL can be effective within certain time ranges of a week. To this end, first you must configure a time range, then you can configure relevant time control in time range configuration mode.

Configuring Absolute Time Range

Command	**absolute** { [**start** *time date*] | [**end** *time date*] }
Parameter Description	**start** *time date*: start time of the range. **end** *time date*: end time of the range.
Command Mode	Time range configuration mode
Usage Guide	Use the **absolute** command to configure a time absolute time range between a start time and an end time to allow a certain function to take effect within the absolute time range.

Configuring Periodic Time

Command	**periodic** *day-of-the-week time* **to** [*day-of-the-week*] *time*
Parameter Description	*day-of-the-week*: the week day when the periodic time starts or ends *time*: the exact time when the periodic time starts or ends
Command Mode	Time range configuration mode
Usage Guide	Use the **periodic** command to configure a periodic time interval to allow a certain function to take effect within the periodic time.

10.5 Monitoring and Maintaining Time Range

Displaying the Running Status

Function	Command
Displays time range configuration.	**show time-range** [*time-range-name*]

11 Configuring SMART-DNS

11.1 Overview

SMART-DNS is a feature that enables an egress gateway in a network with multiple outbound interfaces to smartly respond to domain name system (DNS) resolution requests from external clients of different operator networks based on the route status. SMART-DNS improves service quality of intranet servers.

11.2 Applications

Application	Description
Applying Scenario with Routes of Multiple Operators	The egress gateway connects to different operator networks via different routes. A DNS server is deployed in the intranet along with other servers that externally provide services. External clients access the servers via different routes.

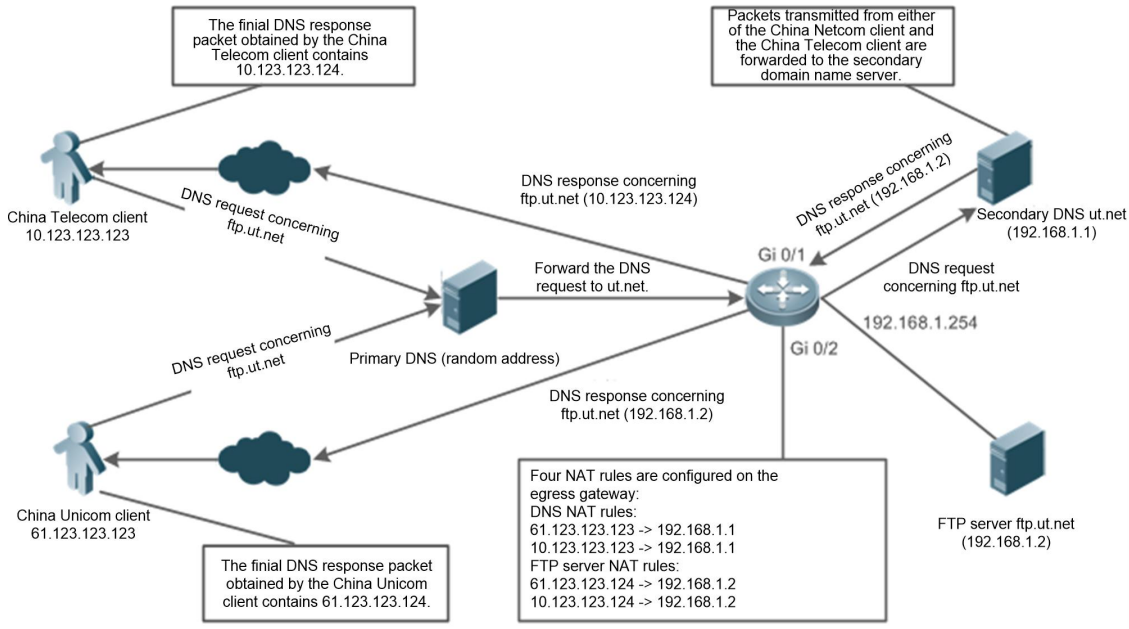
11.2.1 Applying Scenario with Routes of Multiple Operators

Scenario

Two outbound routes exist in the network: route to the China Telecom network and that to the China Netcom network.

- The public IP address of the intranet server obtained by the China Telecom client by DNS resolution is an IP address of a China Telecom network port.
- The public IP address of the intranet server obtained by the China Netcom client by DNS resolution is an IP address of a China Netcom network port.

Figure 10-1



Deployment

- Configure different operators for different routes.
- Deploy a DNS server in the intranet. Enable the extranet client to obtain, by using the DNS server and via resolution, the IP address of an intranet server.

11.3 Features

Basic Concepts

↘ DNS

DNS is a core Internet service. As a distributed database that can map a domain name to an IP address, the DNS facilitates Internet access without memorizing the IP string.

Overview

Feature	Description
SMART-DNS	The DNS response packet returned to the client is modified based on the routing result.

11.3.1 SMART-DNS

Based on the operator to which the client belongs, return a DNS response packet that is destined for the network of the operator.

Working Principle

The egress gateway provides a routing table, and therefore an Internet service provider (ISP) to which a source address belongs can be queried with ease. A DNS response packet returned to the client is modified based on this routing result. In this way, the egress gateway can implement SMART-DNS without generating too many overheads.

Related Configuration

Configuring Route Database for Interface

No route database is configured for any interface by default.

Run the route-auto-choose command to configure a route database for an interface, so that an ISP to which a client belongs can be queried subsequently.

Configuring SMART-DNS

No DNS rule is configured by default.

Run the smartdns command to configure related rules.

11.4 Configuration

Configuration	Description and Command	
Configuring SMART-DNS	(Mandatory) It is used to enable SMART-DNS and configure a SMART-DNS policy.	
	smartdns enable	Enables SMART-DNS.
	smartdns *sip interface* **map** *mip*	Configures a SMART-DNS rule.

11.4.1 Configuring SMART-DNS

Configuration Effect

- Enable SMART-DNS.
- Configure SMART-DNS rules, so that clients belonging to different ISPs obtain, by resolution, different public IP addresses (of the intranet server) that belong to their respective ISPs.

Notes

- To improve SMART-DNS performance, configure the route database function on the corresponding public network interface.

Configuration Steps

Configuring SMART-DNS

- Mandatory.
- Configure SMART-DNS in global configuration mode.

Verification

Set up an environment with two outbound interfaces: one for the China Telecom network and the other for the education network. Set up a DNS server and specific service servers (such as the FTP server) on the intranet, and ensure that the servers can be queried from an external network. Configure corresponding SMART-DNS rules.

- The service server IP address obtained by the China Telecom client is an IP address of the China Telecom outbound interface.
- The service server IP address obtained by the education network client is an IP address of the education network outbound interface.

Related Commands

Enabling SMART-DNS

Command	[no] smartdns enable
Parameter Description	**enable**: Enables SMART-DNS.
Command Mode	Global configuration mode
Usage Guide	N/A

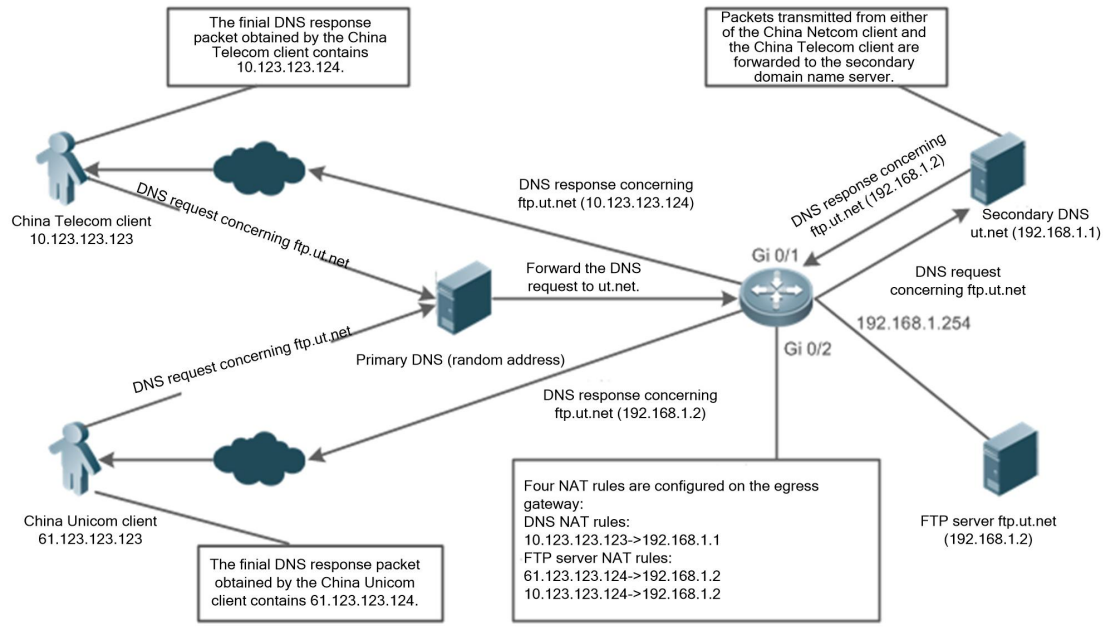
Configuring SMART-DNS Rules

Command	[no] smartdns *sip interface* map *mip*
Parameter Description	*sip*: Indicates the intranet server IP address. Interface: Indicates the interface on which the source IP address is translated into mapped IP address. **map**: Indicates mapping. *mip*: Indicates the public IP address of the service server.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

The following example describes only configuration related to SMART-DNS.

Enabling China Telecom Client and China Netcom Client to Access Intranet FTP Server Respectively via China Telecom Outbound Interface gi0/1 and China Netcom Outbound Interface gi0/2

Scenario Figure 10-2	
Configuration Steps	● Enable SMART-DNS and configure two corresponding SMART-DNS rules.
A	A# configure terminal A(config)# smartdns enable A(config)# smartdns 192.168.1.2 gigabitEthernet 0/1 map 10.123.123.124 A(config)# smartdns 192.168.1.2 gigabitEthernet 0/2 map 61.123.123.124
Verification	Verify that the China Telecom client access ftp.ut.net via the IP address 10.123.123.124, and that the China Netcom client access ftp.ut.net via the address 61.123.123.124. ● Run the show command to check whether the configuration is successful.
A	A# show smartdns config smartdns：enable cli: smartdns 192.168.1.2 Gi0/1 map 10.123.123.124 smartdns 192.168.1.2 Gi0/2 map 10.123.123.124

Common Errors

- No route database is configured, causing a routing error.

11.5 Monitoring

Displaying

Description	Command
Displays the SMART-DNS configuration.	**show smartdns config**

Chapter 3 Basic Management

1. Configuring CLI
2. Configuring Basic Management
3. Configuring Lines
4. Configuring Password Policy
5. Configuring Software Authorization Management
6. Configuring PKG_MGMT
7. Configuring CWMP
8. Configuring Syslog
9. Configuring LED
10. Configuring Exception Alarm
11. Configuring HTTP Service
12. Configuring Patch Upgrade
13. Configuring Web Upgrade

1 Configuring CLI

1.1 Overview

The command line interface (CLI) is a window used for text command interaction between users and network devices. You can enter commands in the CLI window to configure and manage network devices.

Protocols and Standards

N/A

1.2 Applications

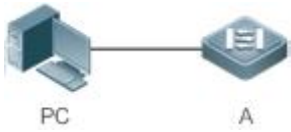
Application	Description
Configuring and Managing Network Devices Through CLI	You can enter commands in the CLI window to configure and manage network devices

1.2.1 Configuring and Managing Network Devices Through CLI

Scenario

As shown in Figure 1- 1, a user accesses network device A using a PC, and enter commands in the CLI window to configure and manage the network device.

Figure 1- 1

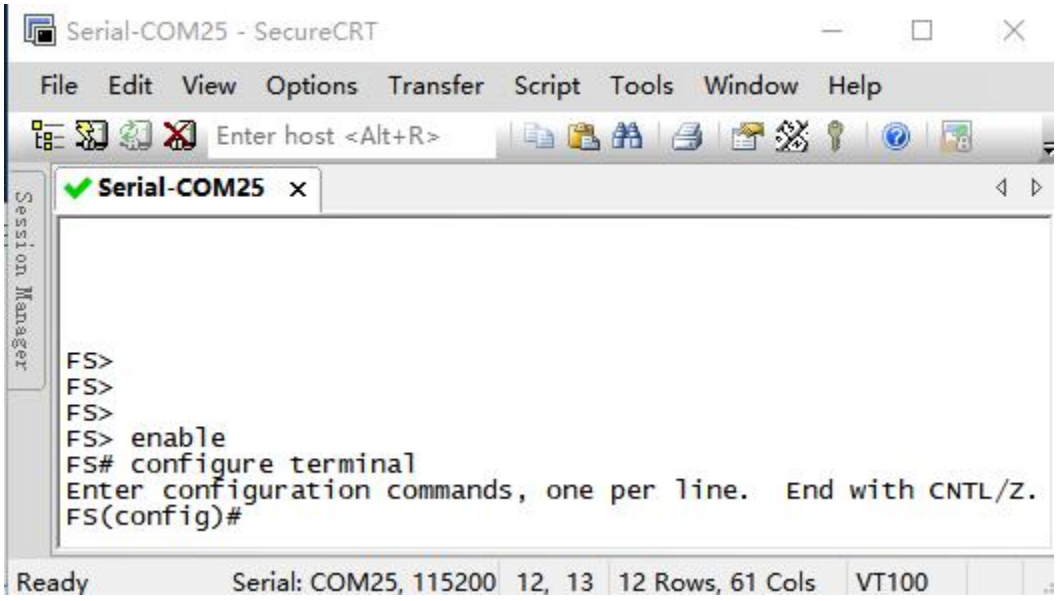


Remarks	A is the network device to be managed. PC is a terminal.

Deployment

As shown in Figure 1- 2, the user uses the Secure CRT installed on a PC to set up a connection with network device A, and opens the CLI window to enter configuration commands.

Figure 1- 2



1.3 Features

Overview

Feature	Description
Accessing CLI	You can log in to a network device for configuration and management.
Command Modes	The CLI provides several command modes. Commands that can be used vary according to command modes.
System Help	You can obtain the help information of the system during CLI configuration.
Abbreviated Commands	If the entered string is sufficient to identify a unique command, you do not need to enter the full string of the command.
No and Default Options of Commands	You can use the **no** option of a command to disable a function or perform the operation opposite to the command, or use the **default** option of the command to restore default settings.
Prompts Indicating Incorrect Commands	An error prompt will be displayed if an incorrect command is entered.
History Commands	You can use short-cut keys to display or call history commands.
Featured Editing	The system provides short-cut keys for editing commands.
Searching and Filtering of the Show Command Output	You can run the **show** command to search or filter specified commands.
Command Alias	You can configure alias of a command to replace the command.

1.3.1 Accessing CLI

Before using the CLI, you need to connect a terminal or PC to a network device. You can use the CLI after starting the network device and finishing hardware and software initialization. When used for the first time, the network device can be connected only through the

console port, which is called out band management. After performing relevant configuration, you can connect and manage the network device through Telnet.

1.3.2 Command Modes

Due to the large number of commands, these commands are classified by function to facilitate the use of commands. The CLI provides several commands modes, and all commands are registered in one or several command modes. You must first enter the command mode of a command before using this command. Different command modes are related with each other while distinguished from each other.

As soon as a new session is set up with the network device management interface, you enter User EXEC mode. In this mode, you can use only a small number of commands and the command functions are limited, such as the **show** commands. Execution results of commands in User EXEC mode are not saved.

To use more commands, you must first enter Privileged EXEC mode. Generally, you must enter a password to enter Privileged EXEC mode. In Privileged EXEC mode, you can use all commands registered in this command mode, and further enter global configuration mode.

Using commands of a certain configuration mode (such as global configuration mode and interface configuration mode) will affect configuration in use. If you save the configuration, these commands will be saved and executed next time the system is restarted. You must enter global configuration mode before entering another configuration mode, such as interface configuration mode.

The following table summarizes the command modes by assuming that the name of the network device is "FS".

Command Mode	Access Method	Prompt	Exit or Entering Another Mode	About
User EXEC (User EXEC mode)	Enter User EXEC mode by default when accessing a network device.	FS>	Run the **exit** command to exit User EXEC mode. Run the **enable** command to enter Privileged EXEC mode.	Use this command mode to conduct basic tests or display system information.
Privileged EXEC (Privileged EXEC mode)	In User EXEC mode, run the **enable** command to enter Privileged EXEC mode.	FS#	Run the **disable** command to return to User EXEC mode. Run the **configure** command to enter global configuration mode.	Use this command mode to check whether the configuration takes effect. This mode is password protected.
Global configuration (Global configuration mode)	In Privileged EXEC mode, run the **configure** command to enter global configuration mode.	FS(config)#	Run the **exit** or **end** command, or press **Ctrl+C** to return to Privileged EXEC mode. Run the **interface** command to enter interface configuration mode. When using the **interface** command, you must specify the interface. Run the **vlan** *vlan_id* command to enter VLAN configuration mode.	Using commands in this mode will affect the global parameters of the network device.

Command Mode	Access Method	Prompt	Exit or Entering Another Mode	About
Interface configuration (Interface configuration mode)	In global configuration mode, run the **interface** command to enter interface configuration mode.	FS(config-if)#	Run the **end** command, or press **Ctrl+C** to return to Privileged EXEC mode. Run the **exit** command to return to global configuration mode. When using the **interface** command, you must specify the interface.	Use this configuration mode to configure various interfaces of the network device.
Config-vlan (VLAN configuration mode)	In global configuration mode, run the **vlan** *vlan_id* command to enter VLAN configuration mode.	FS(config-vlan)#	Run the **end** command, or press **Ctrl+C** to return to the Privileged EXEC mode. Run the **exit** command to return to global configuration mode.	Use this configuration mode to configure VLAN parameters.

1.3.3 System Help

When entering commands in the CLI window, you can obtain the help information using the following methods:

16. At the command prompt in any mode, enter a question mark (?) to list the commands supported by the current command mode and related command description.

For example

```
FS>?
Exec commands:
  <1-99>      Session number to resume
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  help        Description of the interactive help system
  lock        Lock the terminal
  ping        Send echo messages
  show        Show running system information
  telnet      Open a telnet connection
  traceroute  Trace route to destination
```

17. Enter a space and a question mark (?) after a keyword of a command to list the next keyword or variable associated with the keyword.

For example

```
FS(config)#interface ?
  Aggregateport       Aggregate port interface
  Dialer              Dialer interface
  GigabitEthernet     Gigabit Ethernet interface
  Loopback            Loopback interface
  Multilink           Multilink-group  interface
  Null                Null interface
  Tunnel              Tunnel interface
  Virtual-ppp         Virtual PPP interface
  Virtual-template    Virtual Template interface
  Vlan                Vlan interface
  range               Interface range command
```

If the keyword is followed by a parameter value, the value range and description of this parameter are displayed as follows:

```
FS(config)#interface vlan ?
  <1-4094>   Vlan port number
```

18. Enter a question mark (?) after an incomplete string of a command keyword to list all command keywords starting with the string.

For example

```
FS#d?
debug   delete   diagnostic   dir   disable   disconnect
```

19. After an incomplete command keyword is entered, if the suffix of this keyword is unique, press the **Tab** key to display the complete keyword.

For example

```
FS# show conf<Tab>
FS# show configuration
```

20. In any command mode, run the **help** command to obtain brief description about the help system.

For example

```
FS(config)#help
Help may be requested at any point in a command by entering
a question mark '?'.   If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
```

```
    argument.
2. Partial help is provided when an abbreviated argument is entered
    and you want to know what arguments match the input
    (e.g. 'show pr?'.)
```

1.3.4 Abbreviated Commands

If a command is long, you can enter a part of the command that is sufficient to identify the command keyword.

For example, to run the **interface** *gigabitEthernet 0/1* command in GigabitEthernet 0/1 interface configuration mode, enter the abbreviated command as follows:

```
FS(config)#int g0/1
FS(config-if-GigabitEthernet 0/1)#
```

1.3.5 No and Default Options of Commands

Most commands have the **no** option. Generally, the **no** option is used to disable a feature or function, or perform the operation opposite to the command. For example, run the **no shutdown** command to perform the operation opposite to the **shutdown** command, that is, enabling the interface. The keyword without the **no** option is used to enable a disabled feature or a feature that is disabled by default.

Most configuration commands have the **default** option. The **default** option is used to restore default settings of the command. Default values of most commands are used to disable related functions. Therefore, the function of the **default** option is the same as that of the **no** option in most cases. For some commands, however, the default values are used to enable related functions. In this case, the function of the **default** option is opposite to that of the **no** option. At this time, the **default** option is used to enable the related function and set the variables to default values.

For specific function of the **no** or **default** option of each command, see the command reference.

1.3.6 Prompts Indicating Incorrect Commands

When you enter an incorrect command, an error prompt is displayed.

The following table lists the common CLI error messages.

Error Message	Meaning	How to Obtain Help
% Ambiguous command: "show c"	The characters entered are insufficient for identifying a unique command.	Re-enter the command, and enter a question mark after the word that is ambiguous. All the possible keywords will be displayed.
% Incomplete command.	The mandatory keyword or variable is not entered in the command.	Re-enter the command, and enter a space and a question mark. All the possible keywords or variables will be displayed.
% Invalid input detected at '^' marker.	An incorrect command is entered. The sign (^) indicates the position of the word that causes the error.	At the current command mode prompt, enter a question mark. All the command keywords allowed in this command mode will be displayed.

1.3.7 History Commands

The system automatically saves commands that are entered recently. You can use short-cut keys to display or call history commands.

The methods are described in the following table.

Operation	Result
Ctrl+P or the UP key	Display the previous command in the history command list. Starting from the latest record, you can repeatedly perform this operation to query earlier records.
Ctrl+N or the DOWN key	After pressing Ctrl+N or the DOWN key, you can return to a command that is recently executed in the history command list. You can repeatedly perform this operation to query recently executed commands.

The standard terminals, such as the VT100 series, support the direction keys.

1.3.8 Featured Editing

When editing the command line, you can use the keys or short-cut keys listed in the following table:

Function	Key or Short-Cut Key	Description
Move the cursor on the editing line.	Left key or Ctrl+B	Move the cursor to the previous character.
	Right key or Ctrl+B	Move the cursor to the next character.
	Ctrl+A	Move the cursor to the head of the command line.
	Ctrl+E	Move the cursor to the end of the command line.
Delete an entered character.	Backspace key	Delete one character to the left of the cursor.
	Delete key	Delete one character to the right of the cursor.
Move the output by one line or one page.	Return key	When displaying contents, press the **Return** key to move the output one line upward and display the next line. This operation is performed when the output does not end yet.
	Space key	When displaying contents, press the **Space** key to page down and display the next page. This operation is performed when the output does not end yet.

When the editing cursor is close to the right boundary, the entire command line will move to the left by 20 characters, and the hidden front part is replaced by the dollar ($) signs. You can use the related keys or short-cut keys to move the cursor to the characters in the front or return to the head of the command line.

For example, the whole **access-list** may exceed the screen width. When the cursor is close to the end of the command line for the first time, the entire command line moves to the left by 20 characters, and the hidden front part is replaced by the dollar signs ($). Each time the cursor is close to the right boundary, the entire command line moves to the left by 20 characters.

```
access-list 199 permit ip host 192.168.180.220 host
$ost 192.168.180.220 host 202.101.99.12
$0.220 host 202.101.99.12 time-range tr
```

Press **Ctrl+A** to return to the head of the command line. At this time, the hidden tail part of the command line is replaced by the dollar signs ($).

```
access-list 199 permit ip host 192.168.180.220 host 202.101.99.$
```

The default screen width is 80 characters.

1.3.9 Searching and Filtering of the Show Command Output

To search specified contents from the output of the **show** command, run the following command:

Command	Description
show *any-command* | **begin** *regular-expression*	Searches specified contents from the output of the **show** command. The first line containing the contents and all information that follows this line will be output.

The **show** command can be executed in any mode.

Searched contents are case sensitive.

To filter specified contents from the output of the **show** command, run the following commands:

Command	Description
show *any-command* | **exclude** *regular-expression*	Filters the output of the **show** command. Except those containing the specified contents, all lines will be output.
show *any-command* | **include** *regular-expression*	Filters the output of the **show** command. Only the lines containing the specified contents will be output.

To search or filter the output of the **show** command, you must enter a vertical line (|). After the vertical line, select the searching or filtering rules and contents (character or string). Searched and filtered contents are case sensitive.

```
FS#show running-config | include interface
interface GigabitEthernet 0/0
interface GigabitEthernet 0/1
interface GigabitEthernet 0/2
interface GigabitEthernet 0/3
interface GigabitEthernet 0/4
interface GigabitEthernet 0/5
interface GigabitEthernet 0/6
interface GigabitEthernet 0/7
interface Mgmt 0
```

1.3.10 Command Alias

You can configure any word as the alias of a command to simply the command input.

Configuration Effect

1. Replace a command with a word.

For example, configure "mygateway" as the alias of the **ip route** *0.0.0.0 0.0.0.0192.1.1.1* command. To run this command, you only need to enter "mygateway".

2. Replace the front part of a command with a word, and enter the later part.

For example, configure "ia" as the alias of the **ip address** command. To run this command, you need to enter "ia" and then the specified IP address and subnet mask.

Configuration Steps

Displaying Default Alias

In User EXEC or Privileged EXEC mode, default alias are available for some commands. You can run the **show aliases** command to display these default aliases.

```
FS(config)#show aliases
Exec mode alias:
  h                    help
  p                    ping
  s                    show
  u                    undebug
  un                   undebug
```

These default aliases cannot be deleted.

Configuring a Command Alias

Command	**alias** *mode command-alias original-command*
Parameter Description	*mode*: indicates the command mode of the command represented by the alias. *command-alias*: indicates the command alias. *original-command*: indicates the command represented by the alias.
Command Mode	Global configuration mode
Usage Guide	In global configuration mode, run the **alias** ? command to list all command modes that can be configured with aliases.

Displaying Settings of Command Aliases

Run the **show aliases** command to display alias settings in the system.

Notes

- The command replaced by an alias must start from the first character of the command line.
- The command replaced by an alias must be complete.
- The entire alias must be entered when the alias is used; otherwise, the alias cannot be identified.

Configuration Example

Defining an Alias to Replace the Entire Command

Configuration Steps	In global configuration mode, configure the alias "ir" to represent the default route configuration command **ip route** *0.0.0.0 0.0.0.0 192.168.1.1.*
	FS#configure terminal FS(config)#alias config ir ip route 0.0.0.0 0.0.0.0 192.168.1.1
Verification	● Run the **show alias** command to check whether the alias is configured successfully. FS(config)#show alias Exec mode alias: h help p ping s show u undebug un undebug Global configuration mode alias: ir ip route 0.0.0.0 0.0.0.0 192.168.1.1
	● Use the configured alias to run the command, and run the **show running-config** command to check whether the alias is configured successfully.
	FS(config)#ir FS(config)#show running-config Building configuration… ! alias config ir ip route 0.0.0.0 0.0.0.0 192.168.1.1 //Configuring an alias … ip route 0.0.0.0 0.0.0.0 192.168.1.1 //Configuration result after the alias "ir" is entered !

Defining an Alias to Replace the Front Part of a Command

Configuration Steps	In global configuration mode, configure the alias "ir" to represent the front part "**ip route**" of the default route configuration command.
	FS#configure terminal

	FS(config)#alias config ir ip route
Verification	● Run the **show alias** command to check whether the alias is configured successfully. FS(config)#show alias Exec mode alias: h help p ping s show u undebug un undebug Global configuration mode alias: ir ip route
	● Enter the alias "ir" and then the later part of the command "0.0.0.0 0.0.0.0 192.168.1.1". ● Run the **show ap-config running** command to check whether the configuration is successful.
	FS(config)#ir 0.0.0.0 0.0.0.0 192.168.1.1 FS(config)#show running Building configuration… ! alias config ir ip route //Configuring an alias ! ip route 0.0.0.0 0.0.0.0 192.168.1.1 //Configuration result after the alias "ir" and the later part of the command are entered !

System Help

1. The system provides help information for command alias. An asterisk (*) will be displayed in front of an alias. The format is as follows:

```
*command-alias=original-command
```

For example, in Privileged EXEC mode, the default command alias "s" represents the **show** keyword. If you enter "s?", the keywords starting by "s" and alias information are displayed.

```
FS#s?
*s=show    show    start-chat    start-terminal-service
```

2. If the command represented by an alias contains more than one word, the command is displayed in a pair of quotation marks.

For example, in Privileged EXEC mode, configure the alias "sv" to replace the **show version** command. If you enter "s?", the keywords starting by "s" and alias information are displayed.

```
FS#s?
*s=show    *sv=”show version” show    start-chat
start-terminal-service
```

3. You can use the alias to obtain help information about the command represented by the alias.

For example, configure the alias "ia" to represent the **ip address** command in interface configuration mode. If you enter "ia?" in interface configuration mode, the help information on "ip address?" is displayed, and the alias is replaced by the command.

```
FS(config-if)#ia ?
  A.B.C.D    IP address
  dhcp       IP Address via DHCP
FS(config-if)#ip address
```

If you enter a space in front of a command, the command represented by this alias will not be displayed.

2 Configuring Basic Management

2.1 Overview

This document is a getting started guide to network device management. It describes how to manage, monitor, and maintain network devices.

2.2 Applications

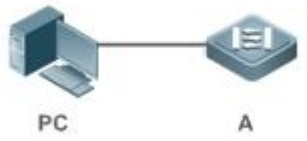
Application	Description
Network Device Management	A user logs in to a network device from a terminal and runs commands on a command line interface (CLI) to manage device configurations.

2.2.1 Network Device Management

Scenario

Network device management described in this document is performed through the CLI. A user logs in to Network Device A from a terminal and runs commands on the CLI to manage device configurations. See Figure 2- 1.

Figure 2- 1



2.3 Features

Basic Concepts

- TFTP

Trivial File Transfer Protocol (TFTP) is a TCP/IP protocol which allows a client to transfer a file to a server or get a file from a server.

- AAA

AAA is short for Authentication, Authorization and Accounting.

Authentication refers to the verification of user identities and the related network services.

Authorization refers to the granting of network services to users according to authentication results.

Accounting refers to the tracking of network service consumption by users. A billing system charges users based on consumption records.

AAA provides effective means of network management and security protection.

- RADIUS

Remote Authentication Dial In User Service (RADIUS) is the most widely used AAA protocol at present.

Telnet

Telnet is a terminal emulation protocol in the TCP/IP protocol stack which provides access to a remote host through a virtual terminal connection. It is a standard protocol located at Layer 7 (application layer) of the Open System Interconnection (OSI) model and used on the internet for remote login. Telnet sets up a connection between the local PC and a remote host.

System Information

System information includes the system description, power-on time, hardware and software versions, control-layer software version, and boot-layer software version.

Hardware Information

Hardware information includes the physical device information as well as slot and module information. The device information includes the device description and slot quantity. The slot information includes the slot ID, module description (which is empty if a slot does not have a module), and actual and maximum number of physical ports.

Overview

Feature	Description
User Access Control	Controls the terminal access to network devices on the internet based on passwords and privileges.
Login Authentication Control	Performs username-password authentication to grant access to network devices when AAA is enabled. (Authentication is performed by a dedicated server.)
Basic System Parameters	Refer to the parameters of a system, such as the clock, banner, and Console baud rate.
Displaying Configurations	Displays the system configurations, including the configurations that the system is currently running and the device configurations stored in the nonvolatile random access memory (NVRAM).
Telnet	Telnet is an application-layer protocol in the TCP/IP protocol stack. It provides the standard governing remote login and virtual terminal communication on the internet.
Restart	Introduces system restart.

2.3.1 User Access Control

User access control refers to the control of terminal access to network devices on the internet based on passwords and privileges.

Working Principle

Privilege Level

16 privilege levels are defined ranging from 0 to 15 for CLI on network devices to grant users access to different commands. Level 0 is the lowest level granting access to just a few commands, whereas level 15 is the highest level granting access to all commands. Levels 0 and 1 are common user levels without the device configuration permission (users are not allowed to enter global configuration mode by default). Levels 2–15 are privileged user levels with the device configuration permission.

Password Classification

Passwords are classified into two types: password and security. The first type refers to simple encrypted passwords at level 15. The second type refers to secure encrypted passwords at levels 0–15. If a level is configured with both simple and secure encrypted passwords, the simple encrypted password will not take effect. If you configure a non-15 level simple encrypted password, a warning is displayed and the password is automatically converted into a secure encrypted password. If you configure the same simple encrypted password and secure encrypted password at level 15, a warning is displayed.

Password Protection

Each privilege level on a network device has a password. An increase in privilege level requires the input of the target level password, whereas a reduction in privilege level does not require password input.

By default, only two privilege levels are password-protected, namely, level 1 (common user level) and level 15 (privileged user level). Sixteen privilege levels with password protection can be assigned to the commands in each mode to grant access to different commands.

If no password is configured for a privileged user level, access to this level does not require password input. It is recommended that a password be configured for security purposes.

Command Authorization

Each command has its lowest execution level. A user with a privilege level lower than this level is not allowed to run the command. After the command is assigned a privilege level, users at this level and higher have access to the command.

Related Configuration

Configuring a Simple Encrypted Password

- Run the enable password command.

Configuring a Secure Encrypted Password

- Run the enable secret command.
- A secure encrypted password is used to control the switching between user levels. It has the same function as a simple encrypted password but uses an enhanced password encryption algorithm. Therefore, secure encrypted passwords are recommended out of security consideration.

Configuring Command Privilege Levels

- Run the privilege command to assign a privilege level to a command.
- A command at a lower level is accessible by more users than a command at a higher level.

Raising/Lowering a User Privilege Level

- Run the enable command or the disable command to raise or lower a user privilege level respectively.
- After logging in to a network device, the user can change his/her level to obtain access to commands at different privilege levels.

Enabling Line Password Protection

- Line password protection is required for remote login (such as login through Telnet).
- Run the password[0 | 7] line command to configure a line password, and then run the login command to enable password protection.

- By default, terminals do not support the lock command.

2.3.2 Login Authentication Control

In login authentication with AAA disabled, the password entered by a user is checked against the configured line password. If they are consistent, the user can access the network device. In local authentication, the username and password entered by a user are checked against those stored in the local user database. If they are matched, the user can access the network device with proper management permissions.

In AAA, the username and password entered by a user are authenticated by a server. If authentication is successful, the user can access the network device and enjoy certain management permissions.

For example, a RADIUS server can be used to authenticate usernames and passwords and control users' management permissions on network devices. Network devices no longer store users' passwords, but send encrypted user information to the RADIUS server, including usernames, passwords, shared passwords, and access policies. This provides a convenient way to manage and control user access and improve user information security.

Working Principle

Line Password

If AAA is disabled, you can configure a line password used to verify user identities during login. After AAA is enabled, line password verification does not take effect.

Local Authentication

If AAA is disabled, you can configure local authentication to verify user identities and control management permissions by using the local user database. After AAA is enabled, local authentication does not take effect.

AAA

AAA provides three independent security functions, namely, Authentication, Authorization and Accounting. A server (or the local user database) is used to perform authentication based on the configured login authentication method list and control users' management permissions. For details about AAA, see *Configuring AAA*.

Related Configuration

Configuring Local User Information

- Run the username command to configure the account used for local identity authentication and authorization, including usernames, passwords, and optional authorization information.

Configuring Local Authentication for Line-Based Login

- Run the login local command (in the case that AAA is disabled).
- Perform this configuration on every device.

Configuring AAA Authentication for Line-Based Login

- The default authentication method is used after AAA is enabled.
- Run the login authentication command to configure a login authentication method list for a line.
- Perform this configuration when the local AAA authentication is required.

Configuring Non-AAA Authentication for Line-Based Login When AAA Is Enabled

- Run the login access non-aaa command in global configuration mode.
- Perform this configuration on every device.

Configuring the Connection Timeout Time

- The default connection timeout time is 10 minutes.
- Run the exec-timeout command to change the default connection timeout time. An established connection will be closed if no output is detected during the timeout time.
- Perform this configuration when you need to increase or reduce the connection timeout time.

Configuring the Session Timeout Time

- The default session timeout time is 0 minutes, indicating no timeout.
- Run the session-timeout command to change the default session timeout time.
- The session established to a remote host through a line will be disconnected if no output is detected during the timeout time. Then the remote host is restored to Idle. Perform this configuration when you need to increase or reduce the session timeout time.

Locking a Session

- By default, terminals do not support the lock command.
- Run the lockable command to lock the terminals connected to the current line.
- To lock a session, first enable terminal lock in line configuration mode, and then run the lock command in terminal EXEC mode to lock the terminal.

2.3.3 Basic System Parameters

System Time

The network device system clock records the time of events on the device. For example, the time shown in system logs is obtained from the system clock. Time is recorded in the format of *year-month-day, hour.minute.second, day of the week*.

When you use a network device for the first time, set its system clock to the current date and time manually.

Configuring a System Name and Command Prompt

You can configure a system name to identify a network device. The default system name is **FS**. A name with more than 32 characters will be truncated to keep only the first 32 characters. The command prompt keeps consistent with the system name.

Banner

A banner is used to display login prompt information. There are two types of banner: Daily notification and login banner.

- Daily notification is displayed on all terminals connected to network devices soon after login. Urgent messages (such as immediate system shutdown) can be delivered to users through daily notification.
- A login banner appears after daily notification to display login information.

Configuring the Console Baud Rate

You can manage network device through a Console port The first configuration on the network device must be performed through the Console port. The serial port baud rate can be changed based on actual requirements. Note that the management terminal must have consistent baud rate setting with the device console.

Configuring the Connection Timeout Time

The connection timeout time is used to control device connections (including established connections and sessions established to remote hosts). A connection will be closed when no input is detected during the timeout time.

Related Configuration

Configuring the System Date and Clock

- Run the clock set command to configure the system time of a network device manually. The device clock starts from the configured time and keeps running even when the device is powered off.

Updating the Hardware Clock

- If the hardware clock and software clock are not synchronized, run the clock update-calendar command to copy the date and time of the software clock to the hardware clock.

Configuring a System Name

- Run the hostname command to change the default system name.
- The default host name is FS.

Configuring a Command Prompt

- Run the prompt command.

Configuring Daily Notification

- By default, no daily notification is configured.
- Run the banner motd command to configure daily notification.
- Daily notification is displayed on all terminals connected to network devices soon after login. Urgent messages (such as immediate system shutdown) can be delivered to users through daily notification.

Configuring a Login Banner

- By default, no login banner is configured.
- Run the banner login command to configure a login banner to display login information.

Configuring the Console Baud Rate

- Run the speed command.
- The default baud rate is 9,600 bps.

2.3.4 Displaying Configurations

Displays the system configurations, including the configurations that the system is currently running and the device configurations stored in the NVRAM.

Working Principle

Running Configurations

Running configurations, namely, running-config, are the configurations that individual component modules run in real time. A request can be made to all running components to collect configurations, which will be orchestrated before being displayed to users. Only running components may provide real-time configurations, whereas unloaded components do not display configurations. In the case that the system is started, a component process is restarted, and a hot patch is executed, the configurations collected during this period may be inaccurate due to the component unstable state. For example, the configurations of a component may not be missing initially but can be displayed later.

Startup Configurations

The configurations stored in the NVRAM, namely, startup-config, are the configurations executed during device startup. When the system is restarted, startup-config is loaded to become new running-config. To display permanent configurations, the system needs to read the **startup-config** file in the NVRAM.

Related Configuration

Displaying Running Configurations

Run the **show running-config** [**interface** *interface*] command to display the configurations that the system is currently running or the configurations on an interface.

Displaying Startup Configurations

Run the **show startup-config** command.

Storing Startup Configurations

Run the **write** or **copy running-config startup-config** command to store the current running configurations as new startup configurations.

2.3.5 Telnet

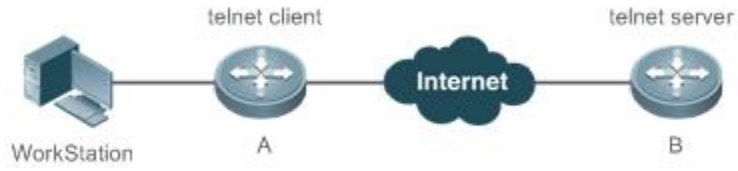
Working Principle

Telnet is an application-layer protocol in the TCP/IP protocol stack. It provides the standard governing remote login and virtual terminal communication on the internet.

The Telnet Client service allows a local or remote user who has logged in to a network device to use its Telnet Client program to access other remote system resources on the internet. In Figure 2- 2, a user with a PC connects to Network Device A by using the terminal emulation or Telnet program and then logs in to Network Device B by using the **telnet** command to perform configuration management.

FSTelnet program supports the use of IPv4 addresses. A Telnet server accepts Telnet connection requests that carry IPv4 addresses. A Telnet client can send connection requests to hosts identified by IPv4 addresses.

Figure 2- 2



Related Configuration

Enabling the Telnet Client Service

- Run the telnet command to log in to a remote device.

Enabling the DoTelnet Client Service

- Run the do telnet command to log in to a remote device.

Restoring a Telnet Client Session

- Run the <1-99> command.

Disconnecting a Suspended Telnet Client Session

- Run the disconnect session-id command.

Enabling the Telnet Server Service

- Run the enable service telnet-server command.
- Perform this configuration when you need to enable Telnet login.

2.3.6 Restart

The timed restart feature makes user operation easier in some scenarios (such as tests).

- If you configure a time interval, the system will restart after the interval. The interval is in the format of mmm or hhh:mm, in the unit of minutes. You can specify the interval name to reflect the restart purpose.
- If you define a future time, the system will restart when the time is reached.

The clock feature must be supported by the system if you want to use the **at** option. It is recommended that you configure the system clock in advance. A new restart plan will overwrite the existing one. A restart plan will be invalid if the system is restarted before the plan takes effect.

The span between the restart time and current time must not exceed 31 days, and the restart time must be later than the current system time. After you configure a restart plan, do not to change the system clock; otherwise, the plan may fail (for example, the system time is changed to a time after the restart time.)

Related Configuration

Configuring Restart

- Run the reload command to configure a restart policy.
- Perform this configuration when you need to restart a device at a specific time.

2.4 Configuration

Configuring Passwords and Privileges	(Optional) It is used to configure passwords and command privilege levels.	
	enable password	Configures a simple encrypted password.
	enable secret	Configures a secure encrypted password.
	enable	Raises a user privilege level.
Configuring a Restart Policy	(Optional) It is used to configure a system restart policy.	
	reload	Restarts a device.

2.4.1 Configuring Passwords and Privileges

Configuration Effect

- Configure passwords to control users' access to network devices.
- Assign a privilege level to a command to grant the command access to only the users at or higher than the level.
- Lower the command privilege level to grant more users access to the command.
- Raise the command privilege level to limit the command access to a few users.

Notes

- You can use the password configuration command with the level option to configure a password for a specific privilege level. After you specify the level and the password, the password works for the users who need to access this level.
- By default, no password is configured for any level. The default level is 15.
- If you configure a simple encrypted password with a non-15 level, a warning is displayed and the password is automatically converted into a secure encrypted password.
- The system chooses the secure encrypted password over the simple encrypted password if both of them are configured.

Configuration Steps

Configuring a Simple Encrypted Password

- (Optional) Perform this configuration when you need to establish simple encrypted password verification when users switch between different privilege levels.
- Run the enable password command to configure a simple encrypted password.

Configuring a Secure Encrypted Password

- (Optional) Perform this configuration when you need to establish secure encrypted password verification when users switch between different privilege levels.
- Run the enable secret command to configure a secure encrypted password.

- A secure encrypted password has the same function as a simple encrypted password but uses an enhanced password encryption algorithm. Therefore, secure encrypted passwords are recommended out of security consideration.

Configuring Command Privilege Levels

- Optional.
- A command at a lower level is accessible by more users than a command at a higher level.

Raising/Lowering a User Privilege Level

- After logging in to a network device, the user can change his/her level to obtain access to commands at different privilege levels.
- Run the enable command or the disable command to raise or lower a user privilege level respectively.

Enabling Line Password Protection

- (Optional) Line password protection is required for remote login (such as login through Telnet).
- Run the password [0 | 7] line command to configure a line password, and then run the login command to enable login authentication.

If a line password is configured but login authentication is not configured, the system does not display password prompt.

Verification

- Run the show privilege command to display the current user level.
- Run the show running-config command to display the configuration.

Related Commands

Configuring a Simple Encrypted Password

Command	**enable password** [**level** *level*] { *password* | [**0** | **7**] *encrypted-password* }
Parameter Description	*level:* Indicates a specific user level. *password:* Indicates the password used to enter privileged EXEC mode. *0:* Indicates that the password is entered in plaintext. *7:* Indicates that the password is entered in cyphertext. *encrypted-password:* Indicates the password text, which must contain case-sensitive English letters and digits. Leading spaces are allowed, but will be ignored. However, intermediate and trailing spaces are recognized.
Command Mode	Global configuration mode
Usage Guide	Currently, simple encrypted passwords can be configured with only level 15 and take effect only when no secure encrypted password is configured. If you configure a simple encrypted password with a non-15 level, a warning is displayed and the password is automatically converted into a secure encrypted password. If the level 15 simple encrypted password and secure encrypted password are configured the same, a warning is displayed. If you specify an encryption type and enter a password in plaintext, you cannot re-enter privileged EXEC mode.

	An encrypted password cannot be retrieved once lost. You have to configure a new password.

Configuring a Secure Encrypted Password

Command	**enable secret** [**level** *level*] {*secret* | [**0** | **5**] *encrypted-secret* }
Parameter Description	*level*: Indicates a specific user level. secret: Indicates the password used to enter privileged EXEC mode. **0** | **5**: Indicates the password encryption type. 0 indicates no encryption, and 5 indicates secure encryption. *encrypted-password*: Indicates the password text.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure passwords for different privilege levels.

Raising a User Privilege Level

Command	**enable** [*privilege-level*]
Parameter Description	*privilege-level*: Indicates a specific privilege level.
Command Mode	Privileged EXEC mode
Usage Guide	An increase in privilege level requires the input of the target level password.

Lowering a User Privilege Level

Command	**disable** [*privilege-level*]
Parameter Description	*privilege-level*: Indicates a specific privilege level.
Command Mode	Privileged EXEC mode
Usage Guide	A reduction in privilege level does not require password input. Use this command to exit Privileged EXEC mode and return to user EXEC mode. If *privilege-level* is specified, the current privilege level is reduced to the specified level. *privilege-level* must be lower than the current level.

Configuring Command Privilege Levels

Command	**privilege** *mode* [**all**] { **level** *level* | **reset** } *command-string*
Parameter Description	*mode*: Indicates the CLI mode of the command. For example, **config** indicates the global configuration mode, **EXEC** indicates the privileged command mode, and **interface** indicates the interface configuration mode. **all**: Changes the subcommand privilege levels of a specific command to the same level. **level** *level*: Indicates a privilege level, ranging from 0 to 15.

	reset: Restores the command privilege level to the default. *command-string*: Indicates the command to be assigned a privilege level.
Command Mode	Global configuration mode
Usage Guide	To restore a command privilege level, run the **no privilege** *mode* [**all**] **level** *level command* command in global configuration mode.

Specifying a Line Password

Command	**password**[**0** | **7**] *line*
Parameter Description	**0**: Indicates to configure a password in plaintext. **7**: Indicates to configure a password in cyphertext. line: Indicates the password string.
Command Mode	Line configuration mode
Usage Guide	N/A

Enabling Line Password Protection

Command	**login**
Parameter Description	N/A
Command Mode	Line configuration mode
Usage Guide	N/A

Configuration Example

Configuring Command Authorization

Scenario	Assign privilege level 1 to the **reload** command and its subcommands and configure level 1 as the valid level (by configuring the **test** password).
Configuration Steps	● Assign privilege level 1 to the **reload** command and its subcommands.
	FS# configure terminal FS(config)# privilege exec all level 1 reload FS(config)# enable secret level 1 0 test FS(config)# end

Verification	● Check whether the **reload** command and its subcommands are accessible at level 1.
	FS# disable 1 FS> reload ? at reload at<cr>

2.4.2 Configuring Login and Authentication

Configuration Effect

- Establish line-based login identity authentication.
- Run the telnet command on a network device to log in to a remote device.
- Close an established connection if no output is detected during the timeout time.
- Disconnect an established session connecting to a remote host and restore the host to Idle if no output is detected during the timeout time.
- Lock a terminal to deny access. When a user enters any character on the locked terminal, the password prompt is displayed. The terminal will be automatically unlocked if the entered password is correct.

Configuration Steps

Configuring Local User Information

- Mandatory.
- Run the username command to configure the account used for local identity authentication and authorization, including usernames, passwords, and optional authorization information.
- Perform this configuration on every device.

Configuring Local Authentication for Line-Based Login

- Mandatory.
- Configure local authentication for line-based login in the case that AAA is disabled.
- Perform this configuration on every device.

Configuring AAA Authentication for Line-Based Login

- (Optional) Perform this configuration to configure AAA authentication for line-based login.
- Configure AAA authentication for line-based login in the case that AAA is enabled.
- Perform this configuration on every device.

Configuring Non-AAA Authentication for Line-Based Login When AAA Is Enabled

- Optional.
- Run the login access non-aaa command in global configuration mode to authenticate line-based login in non-AAA mode in the case that AAA is enabled.
- Perform this configuration on every device.

Enabling the Telnet Client Service

- Run the telnet command to log in to a remote device.

Enabling the DoTelnet Client Service

- Run the do telnet command to log in to a remote device.

Restoring a Telnet Client Connection

- (Optional) Perform this configuration to restore the connection on a Telnet client.

Closing a Suspended Telnet Client Connection

- (Optional) Perform this configuration to close the suspended connection on a Telnet client.

Enabling the Telnet Server Service

- Optional.
- Enable the Telnet Server service when you need to enable Telnet login.

Configuring the Connection Timeout Time

- Optional.
- An established connection will be closed if no output is detected during the timeout time.
- Perform this configuration when you need to increase or reduce the connection timeout time.

Configuring the Session Timeout Time

- Optional.
- The session connecting to a remote host will be disconnected and the host be restored to Idle if no output is detected during the timeout time.
- Perform this configuration when you need to increase or reduce the session timeout time.

Locking a Session

- (Optional) Perform this configuration when you need to temporarily exit a session on a device.
- To lock a session, first enable terminal lock in line configuration mode, and then run the lock command to lock the terminal.

Verification

- Run the show running-config command to display the configuration.
- In the case that AAA is disabled, after local user information and line-based local authentication are configured, check whether users are prompted for username and password input for access to the CLI.
- In the case that AAA is enabled, after local user information and local AAA authentication are configured, check whether users are prompted for username and password input for access to the CLI.
- Run the show user command to display the information about the users who have logged in to the CLI.
- Telnet clients can connect to devices enabled with the Telnet Server service.

- When a user presses Enter on a locked CLI, the user is prompted for password input. The session is unlocked only when the entered password is the same as the configured one.
- Run the show sessions command to display every established Telnet client instance.

Related Commands

Configuring Local User Information

Command	**username** *name* [**login mode** { **aux** | **console** | **ssh** | **telnet** }] [**online amount** *number*] [**permission** *oper-mode path*] [**privilege** *privilege-level*] [**reject remote-login**] [**web-auth**] [**pwd-modify**] [**nopassword** | **password** [**0** | **7**] *text-string*]
Parameter Description	*name*: Indicates a user name. **login mode**: Indicates the login mode. **aux**: Sets the login mode to AUX. **console**: Sets the login mode to Console. **ssh**: Sets the login mode to SSH. **telnet**: Sets the login mode to Telnet. **online amount** *number*: Indicates the maximum number of online accounts. **permission** *oper-mode path*: Configures the file operation permission. *op-mode* indicates the operation mode, and *path* indicates the directory or path of a specific file. **privilege** *privilege-level*: Indicates the account privilege level, ranging from 0 to 15. **reject remote-login**: Rejects remote login by using the account. **web-auth**: Allows only Web authentication for the account. **pwd-modify**: Allows the account owner to change the password. This option is available only when **web-auth** is configured. **nopassword**: Indicates that no password is configured for the account. **password** [**0** | **7**] *text-string*: Indicates the password configured for the account. 0 indicates that the password is input in plaintext, and 7 indicates that the password is input in cyphertext. The default is plaintext.
Command Mode	Global configuration mode
Usage Guide	Use this command to create a local user database to be used by authentication. If the value 7 is selected for the encryption type, the entered cyphertext string must consist of an even number of characters. This setting is applicable to the scenario where encrypted passwords may be copied and pasted. In other cases, the value 7 is not selected.

Configuring Local Authentication for Line-Based Login

Command	**login local**
Parameter Description	N/A
Command	Line configuration mode

Mode	
Usage Guide	Use this command to configure local authentication for line-based login in the case that AAA is disabled. Local user information is configured by using the **username** command.

Configuring AAA Authentication for Line-Based Login

Command	**login authentication** { **default** | *list-name* }
Parameter Description	**default:** Indicates the default authentication method list name. *list-name*: Indicates the optional method list name.
Command Mode	Line configuration mode
Usage Guide	Use this command to configure AAA authentication for line-based login in the case that AAA is enabled. The AAA authentication methods, including RADIUS authentication, local authentication, and no authentication, are used during the authentication process.

Configuring Non-AAA Authentication for Line-Based Login When AAA Is Enabled

Command	**login access non-aaa**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command when you need to perform non-AAA authentication on line-based login in the case that AAA is enabled. The configuration takes effect for all terminals.

Enabling the Telnet Client Service

Command	**telnet** [**oob**] *host* [*port*] [**/source** { **ip** *A.B.C.D* | **interface** *interface-name* }]
Parameter Description	**oob:** Remotely connects to a Telnet server through out-of-band communication (by using a management port). This option is available only when the device has a management port. *host*: Indicates the IPv4 address, IPv6 address, or host name of the Telnet server. *port*: Indicates the TCP port number of the Telnet server. The default value is 23. **/source:** Indicates the source IP address or source port used by a Telnet client. **ip** *A.B.C.D:* Indicates the source IPv4 address used by the Telnet client. **interface** *interface-name*: Indicates the source port used by the Telnet client.
Command Mode	Privileged EXEC mode
Usage Guide	A user can telnet to a remote device identified by an IPv4 host name, IPv4 address

Enabling the DoTelnet Client Service

Command	**do telnet** [**oob**] *host* [*port*] [**/source** { **ip** *A.B.C.D* | **interface** *interface-name* }]
Parameter Description	**oob:** Remotely connects to a Telnet server through out-of-band communication (by using a management port). This option is available only when the device has a management port. *host*: Indicates the IPv4 address, IPv6 address, or host name of the Telnet server. *port*: Indicates the TCP port number of the Telnet server. The default value is 23. **/source:** Indicates the source IP address or source port used by a Telnet client. **ip** *A.B.C.D:* Indicates the source IPv4 address used by the Telnet client. **interface** *interface-name*: Indicates the source port used by the Telnet client.
Command Mode	Privileged EXEC mode/configuration mode/interface configuration mode
Usage Guide	A user can telnet to a remote device identified by an IPv4 host name, IPv4 address.

Restoring a Telnet Client Session

Command	<1-99>
Parameter Description	N/A
Command Mode	User EXEC mode
Usage Guide	Use this command to restore a Telnet client session. A user can press the shortcut key **Ctrl**+**Shift**+**6 X** to temporarily exit the Telnet client session that is established using the **telnet** command, run the **<1-99>** command to restore the session, and run the **show sessions** command to display the session information.

Closing a Suspended Telnet Client Connection

Command	**disconnect** *session-id*
Parameter Description	*session-id*: Indicates the suspended Telnet client session ID.
Command Mode	User EXEC mode
Usage Guide	Use this command to close a specific Telnet client session by entering the session ID.

Enabling the Telnet Server Service

Command	**enable service telnet-server**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to enable the Telnet Server service. The IPv4 services are also enabled after the command is

	executed.

Configuring the Connection Timeout Time

Command	**exec-timeout** *minutes* [*seconds*]
Parameter Description	*minutes*: Indicates the connection timeout time in the unit of minutes. *seconds*: Indicates the connection timeout time in the unit of seconds.
Command Mode	Line configuration mode
Usage Guide	Use this command to configure the timeout time for the established connections on a line. A connection will be closed when no input is detected during the timeout time. To remove the connection timeout configuration, run the **no exec-timeout** command in line configuration mode.

Configuring the Session Timeout Time

Command	**session-timeout** *minutes*[**output**]
Parameter Description	*minutes*: Indicates the session timeout time in the unit of minutes. **output**: Indicates whether to add data output as a timeout criterion.
Command Mode	Line configuration mode
Usage Guide	Use this command to configure the timeout time for the remote host sessions on a line. A session will be disconnected when no input is detected during the timeout time. To cancel the session timeout time, run the **no session-timeout** command in line configuration mode.

Enabling Line-Based Terminal Lock

Command	**lockable**
Parameter Description	N/A
Command Mode	Line configuration mode
Usage Guide	N/A

Locking a Terminal Connected to the Current Line

Command	**lock**
Parameter Description	N/A
Command Mode	Line configuration mode
Usage Guide	N/A

Configuration Example

Establishing a Telnet Session to a Remote Network Device

Configuration Steps	● Establish a Telnet session to a remote network device with the IP address 192.168.65.119. ● Run the **telnet** command in privileged EXEC mode, and run the **do telnet** command in privileged EXEC mode/configuration mode/interface configuration mode.
	FS# telnet 192.168.65.119 Trying 192.168.65.119 ... Open User Access Verification Password:
	FS# telnet 2AAA:BBBB::CCCC Trying 2AAA:BBBB::CCCC ... Open User Access Verification Password: FS(config)# do telnet 2AAA:BBBB::CCCC Trying 2AAA:BBBB::CCCC ... Open User Access Verification Password:
Verification	● Check whether the Telnet sessions are established to the remote network devices.

Configuring the Connection Timeout Time

Configuration Steps	● Set the connection timeout time to 20 minutes.
	FS# configure terminal//Enter global configuration mode. FS# line vty 0 //Enter line configuration mode. FS(config-line)#exec-timeout 20 //Set the connection timeout time to 20 minutes.
Verification	● Check whether the connection between a terminal and the local device is closed when no input is detected during the timeout time.

Configuring the Session Timeout Time

Configuration Steps	● Set the session timeout time to 20 minutes.

	FS# configure terminal//Enter global configuration mode.
	FS(config)# line vty 0 //Enter line configuration mode.
	FS(config-line)#session-timeout 20//Set the session timeout time to 20 minutes.

Verification	● Check whether the session between a terminal and the local device is disconnected when no input is detected during the timeout time.

2.4.3 Configuring Basic System Parameters

Configuration Effect

- Configure basic system parameters.

Configuration Steps

Configuring the System Date and Clock

- Mandatory.
- Configure the system time of a network device manually. The device clock starts from the configured time and keeps running even when the device is powered off.

The time configuration is applied only to the software clock if the network device does not provide a hardware clock. The configuration will be invalid when the device is powered off.

Updating the Hardware Clock

- Optional.
- Perform this configuration when you need to copy the date and time of the software clock to the hardware clock so that the hardware clock is synchronized with the software clock.

Configuring a System Name

- (Optional) Perform this configuration to change the default system name.

Configuring a Command Prompt

- (Optional) Perform this configuration to change the default command prompt.

Configuring Daily Notification

- (Optional) Perform this configuration when you need to display important prompts or warnings to users.
- You can configure notification in one or multiple lines, which will be displayed to users after login.

Configuring a Login Banner

- (Optional) Perform this configuration when you need to display important messages to users upon login or logout.

Configuring the Console Baud Rate

- (Optional) Perform this configuration to change the default Console baud rate.

Verification

- Run the show clock command to display the system time.
- Check whether a login banner is displayed after login.
- Run the show version command to display the system information and version.

Related Commands

Configuring the System Date and Clock

Command	**clock set** *hh:mm:ss month day year*
Parameter Description	*hh:mm:ss*: Indicates the current time, in the format of *hour* (24-hour format):*minute*:*second*. *day*: Indicates a day (1–31) of the month. *month*: Indicates a month (from January to December) of the year. *year*: Indicates a year, ranging from 1993 to 2035. Abbreviation is not supported.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to configure the system time. If the device does not provide a hardware clock, the time configuration will be invalid when the device is powered off.

Updating the Hardware Clock

Command	**clock update-calendar**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	After the configuration, the time of the software clock will overwrite that of the hardware clock.

Configuring a System Name

Command	**hostname** *name*
Parameter Description	*name*: Indicates the system name, which must consist of printable characters and must not exceed 63 bytes.
Command Mode	Global configuration mode
Usage Guide	To restore the system name to the default, run the **no hostname** command in global configuration mode.

Configuring a Command Prompt

Command	**prompt** *string*
Parameter	*string*: Indicates the command prompt name. A name with more than 32 characters will be truncated to keep only the

Description	first 32 characters.
Command Mode	Privileged EXEC mode
Usage Guide	To restore the command prompt to the default settings, run the **no prompt** command in global configuration mode.

Configuring Daily Notification

Command	**banner motd** *c message c*
Parameter Description	*c*: Indicates a delimiter, which can be any character, such as "&".
Command Mode	Global configuration mode
Usage Guide	A message must start and end with delimiter+carriage return respectively. Any characters following the ending delimiter will be dropped. Any letter contained in the message must not be used as the delimiter. The message must not exceed 255 bytes.

Configuring a Login Banner

Command	**banner login** *c message c*
Parameter Description	*c*: Indicates a delimiter, which can be any character, such as "&".
Command Mode	Global configuration mode
Usage Guide	A message must start and end with delimiter+carriage return respectively. Any characters following the ending delimiter will be dropped. Any letter contained in the message must not be used as the delimiter. The message must not exceed 255 bytes. To remove the login banner configuration, run the **no banner login** command in global configuration mode.

Configuring the Console Baud Rate

Command	**speed** *speed*
Parameter Description	*speed*: Indicates the console baud rate, in the unit of bps. The serial port baud rate can be set to 9,600 bps, 19,200 bps, 38,400 bps, 57,600 bps, or 115,200 bps. The default is 9,600 bps.
Command Mode	Line configuration mode
Usage Guide	You can configure the asynchronous line baud rate based on requirements. The **speed** command is used to configure receive and transmit rates for the asynchronous line.

Configuration Example

Configuring the System Time

Configuration Steps	● Change the system time to 2003-6-20, 10:10:12.
	FS# clock set 10:10:12 6 20 2003 //Configure the system time and date.
Verification	● Run the **show clock** command in privileged EXEC mode to display the system time.
	FS# show clock //Confirm that the changed system time takes effect. clock: 2003-6-20 10:10:54

Configuring Daily Notification

Configuration Steps	● Configure the daily notification message "Notice: system will shutdown on July 6th." with the pound key (#) as the delimiter.
	FS(config)# banner motd #//Starting delimiter Enter TEXT message. End with the character '#'. Notice: system will shutdown on July 6th.# //Ending delimiter FS(config)#
Verification	● Run the **show running-config** command to display the configuration. ● Connect to the local device through the Console, Telnet or SSH, and check whether daily notification is displayed before the CLI appears.
	C:\>telnet 192.168.65.236 Notice: system will shutdown on July 6th. Access for authorized users only. Please enter your password. User Access Verification Password:

Configuring a Login Banner

Configuration Steps	● Configure the login banner message "Access for authorized users only. Please enter your password." with the pound key (#) as the delimiter.
	FS(config)# banner login #//Starting delimiter Enter TEXT message. End with the character '#'. Access for authorized users only. Please enter your password. # //Ending delimiter FS(config)#

Verification	● Run the **show running-config** command to display the configuration. ● Connect to the local device through the Console, Telnet or SSH, and check whether the login banner is displayed before the CLI appears.
	C:\>telnet 192.168.65.236 Notice: system will shutdown on July 6th. Access for authorized users only. Please enter your password. User Access Verification Password:

Configuring the Serial Port Baud Rate

Configuration Steps	● Set the serial port baud rate to 57,600 bps.

	FS# configure terminal //Enter global configuration mode.
	FS(config)# line console 0 //Enter console line configuration mode.
	FS(config-line)# speed 57600 //Set the console baud rate to 57,600 bps.
	FS(config-line)# end //Returns to privileged mode.

Verification	● Run the **show** command to display the configuration.
	FS# show line console 0 //Displays the console configuration. CON Type speed Overruns * 0 CON 57600 0 Line 0, Location: "", Type: "vt100" Length: 25 lines, Width: 80 columns Special Chars: Escape Disconnect Activation ^^x none ^M Timeouts: Idle EXEC Idle Session never never History is enabled, history size is 10. Total input: 22 bytes Total output: 115 bytes Data overflow: 0 bytes stop rx interrupt: 0 times Modem: READY

2.4.4 Enabling and Disabling a Specific Service

Configuration Effect

- Dynamically adjust system services when the system is running, and enable and disable specific services (SNMP Agent, SSH Server, and Telnet Server).

Configuration Steps

Enabling the SNMP Agent, SSH Server, and Telnet Server Services

- (Optional) Perform this configuration when you need to use these services.

Verification

- Run the show running-config command to display the configuration.
- Run the show services command to display the service Enabled/Disable state.

Related Commands

Enabling the SSH Server, Telnet Server, and SNMP Agent Services

Command	**enable service** { **ssh-server** | **telnet-server** | **snmp-agent** }
Parameter Description	**ssh-server:** Enables or disables the SSH Server service. **telnet-server:** Enables or disables the Telnet Server service. **snmp-agent:** Enables or disables the SNMP Agent service.
Command Mode	Global configuration mode
Usage Guide	Use this command to enable and disable specific services.

Configuration Example

Enabling the SSH Server Service

Configuration Steps	● Enable the SSH Server service.
	FS# configure terminal //Enter global configuration mode. FS(config)#enable service ssh-server //Enable the SSH Server service.
Verification	● Run the **show running-config** command to display the configuration. ● Run the **show ip ssh** command to display the configuration and running state of the SSH Server service.

2.4.5 Configuring a Restart Policy

Configuration Effect

Configure a restart policy to restart a device as scheduled.

Configuration Steps

Configuring Direct Restart

Run the **reload** command in privileged EXEC mode to restart the system immediately.

Configuring Timed Restart

```
reload  at  hh:mm:ss month day year
```

If you configure a specific time, the system will restart at the time. The time must be a time in the future. The **month day year** parameter is optional. If it is not specified, the system clock time is used by default.

The clock feature must be supported by the system if you want to use the **at** option. It is recommended that you configure the system clock in advance. A new restart plan will overwrite the existing one. A restart plan will be invalid if the system is restarted before the plan takes effect.

The restart time must be later than the current system time. After you configure a restart plan, do not change the system clock; otherwise, the plan may fail (for example, the system time is changed to a time after the restart time.)

Related Commands

Restarting a Device

Command	**reload** [**at** { *hh* [:*mm* [:*ss*]] } [*month* [*day* [*year*]]]]
Parameter Description	**at** *hh:mm:ss*: Indicates the time when the system will restart. *month*: Indicates a month of the year, ranging from 1 to 12. *day*: Indicates a date, ranging from 1 to 31. *year*: Indicates a year, ranging from 1993 to 2035. Abbreviation is not supported.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to enable a device to restart at a specific time.

2.5 Monitoring

Displaying

Description	Command
show clock	Displays the current system time.
show line { **console** *line-num* | **vty** *line-num* | *line-num* }	Displays line configurations.
show reload	Displays system restart settings.

show running-config [**interface** *interface*]	Displays the current running configurations of the device or the configurations on an interface.
show startup-config	Displays the device configurations stored in the NVRAM.
show this	Displays the current system configurations.
show version [**devices | module | slots**]	Displays system information.
show sessions	Displays the information of each established Telnet client instance.

3 Configuring Lines

3.1 Overview

There are various types of terminal lines on network devices. You can manage terminal lines in groups based on their types. Configurations on these terminal lines are called line configurations. On network devices, terminal lines are classified into multiple types such as CTY, and VTY.

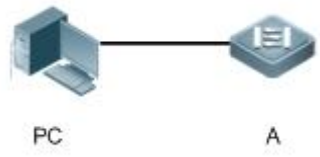
3.2 Applications

Application	Description
Accessing a Device Through Console	Enter the command-line interface (CLI) of a network device through the Console.
Accessing a Device Through VTY	Enter the CLI of a network device through Telnet or SSH.

3.2.1 Accessing a Device Through Console

Scenario

Figure 3- 1



Remarks	A is a network device to be managed. PC is a network management station.

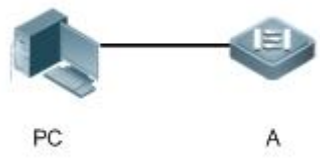
Deployment

The network management station connects to the Console port of a network device through a serial cable. Using the Console software (Hyper Terminal or other terminal simulation software) on the network management station, you can access the Console of the network device and enter the CLI to configure and manage the network device.

3.2.2 Accessing a Device Through VTY

Scenario

Figure 3- 2



Remarks	A is a network device to be managed. PC is a network management station.

Deployment

The network management station connects to a network device through the network. Using a VTY client (such as Putty) on the network management station, you can access the network device through Telnet or SSH and enter the CLI to configure and manage the network device.

3.3 Features

Basic Concepts

↘ CTY

The CTY line refers to the line connected to the Console port. Most network devices have a Console port. You can access the local system through the Console port.

↘ VTY

The VTY line is a virtual terminal line that does not correspond to any hardware. It is used for Telnet or SSH connection.

Overview

Feature	Description
Basic Features	Configures a terminal, displays and clears terminal connection information.

3.3.1 Basic Features

Related Configuration

↘ Configuring Terminal Lines

Run the **line** command in global configuration mode to enter the configuration mode of a specified line.

Configure the line attributes.

↘ Clearing Terminal Connections

When a terminal connects to the network device, the corresponding terminal line is occupied. Run the **show user** command to display the connection status of these terminal lines. If you want to disconnect the terminal from the network device, run the **clear line** command to clear the terminal line. After the terminal lines are cleared, the related connections (such as Telnet and SSH) are interrupted, the CLI exits, and the terminal lines restore to the unoccupied status. Users can re-establish connections.

↘ Specifying the Number of VTY Terminals

Run the **line vty** command to enter the VTY line configuration mode and specify the number of VTY terminals.

By default, there are 5 VTY terminals, numbered from 0 to 4. You can increase the number of VTY terminals to 36, with new ones numbered from 5 to 35. Only new terminals can be removed.

3.4 Configuration

Configuration	Description and Command	
	(Mandatory) It is used to enter the line configuration mode.	
	line [**console** | **vty**] *first-line* [*last-line*]	Enters the specified line configuration mode.
	line vty *line-number*	Increases or reduces the number of available VTY lines.

3.4.1 Entering Line Configuration Mode

Configuration Effect

Enter line configuration mode to configure other functions.

Configuration Steps

Entering Line Configuration Mode

- Mandatory.
- Unless otherwise specified, enter line configuration mode on each device to configure line attributes.

Increasing/Reducing the Number of VTY Lines

- Optional.
- Run the (no) line vty line-number command to increase or reduce the number of VTY lines.

Verification

Run the **show line** command to display line configuration.

Related Commands

Entering Line Configuration Mode

Command	**line** [**console** | **vty**] *first-line* [*last-line*]
Parameter Description	**console**: Indicates the Console port. **vty**: Indicates a virtual terminal line, which supports Telnet or SSH. *first-line*: Indicates the number of the first line. *last-line*: Indicates the number of the last line.
Command Mode	Global configuration mode
Usage Guide	N/A

Increasing/Reducing the Number of VTY Lines

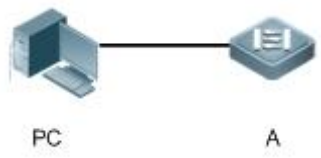
Command	**line vty** *line-number*

Parameter Description	*line-number*: Indicates the number of VTY lines. The value ranges from 0 to 35.
Command Mode	Global configuration mode
Usage Guide	Run the **no line vty** *line-number* command to reduce the number of available VTY lines.

Displaying Line Configuration

Command	**show line** { **console** *line-num* | **vty** *line-num* | *line-num* }
Parameter Description	**console**: Indicates the Console port. **vty**: Indicates a virtual terminal line, which supports Telnet or SSH. *line-num*: Indicates the line to be displayed.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Example

Scenario **Figure 3- 3**	
Configuration Steps	● Connect the PC to network device A through the Console line and enter the CLI on the PC. ● Run the **show user** command to display the connection status of the terminal line. ● Run the **show line console** 0 command to display the status of the Console line. ● Enter global configuration mode and run the **line vty** command to increase the number of VTY terminals to 36.
A	FS#show user Line User Host(s) Idle Location ---------- ---------- ---------- ---------- ---------- * 0 con 0 --- idle 00:00:00 --- FS#show line console 0 CON Type speed Overruns * 0 CON 9600 0

	Line 0, Location: "", Type: "vt100" Length: 24 lines, Width: 79 columns Special Chars: Escape Disconnect Activation ^^x ^D ^M Timeouts: Idle EXEC Idle Session 00:10:00 never History is enabled, history size is 10. Total input: 490 bytes Total output: 59366 bytes Data overflow: 0 bytes stop rx interrupt: 0 times FS#show line vty ? <0-5> Line number FS#configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#line vty 35 FS(config-line)# *Oct 31 18:56:43: %SYS-5-CONFIG_I: Configured from console by console
Verification	● After running the **show line** command, you can find that the number of terminals increases. ● Run the **show running-config** command to display the configuration.
A	FS#show line vty ? <0-35> Line number FS#show running-config Building configuration... Current configuration : 761 bytes version 11.0(1C2B1)(10/16/13 04:23:54 CST -ngcf78) ip tcp not-send-rst

```
vlan 1
!
interface GigabitEthernet 0/0
!
interface GigabitEthernet 0/1
  ip address 192.168.23.164 255.255.255.0
!
interface GigabitEthernet 0/2
!
interface GigabitEthernet 0/3
!
interface GigabitEthernet 0/4
!
interface GigabitEthernet 0/5
!
interface GigabitEthernet 0/6
!
interface GigabitEthernet 0/7
!
interface Mgmt 0
!
line con 0
line vty 0 35
  login
!
end
```

3.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears the line connection status.	**clear line** { **console** *line-num* | **vty** *line-num* | *line-num* }

Displaying

Description	Command
Displays the line configuration.	**show line** { **console** *line-num* | **vty** *line-num* | *line-num* }
Displays historical records of a line.	**show history**
Displays the privilege level of a line.	**show privilege**
Displays users on a line.	**show user** [**all**]

4 Configuring Password Policy

4.1 Overview

The Password Policy is a password security function provided for local authentication of the device. It is configured to control users' login passwords and login states.

The following sections introduce password policy only.

Protocols and Standards

N/A

4.2 Features

Basic Concepts

Minimum Password Length

Administrators can set a minimum length for user passwords according to system security requirements. If the password input by a user is shorter than the minimum password length, the system does not allow the user to set this password but displays a prompt, asking the user to specify another password of an appropriate length.

Strong Password Detection

The less complex a password is, the more likely it is to crack the password. For example, a password that is the same as the corresponding account or a simple password that contains only characters or digits may be easily cracked. For the sake of security, administrators can enable the strong password detection function to ensure that the passwords set by users are highly complex. After the strong password detection function is enabled, a prompt will be displayed for the following types of passwords:

1. Passwords that are the same as corresponding accounts;
2. Simple passwords that contain characters or digits only.

Password Dictionary Detection

The so-called password dictionary is used in combination with password cracking software. It contains many conventional passwords, and therefore improves the cracking rate and shortens the time taken to crack a password.

The password dictionary detects the input password and prevents the user from configuring any password contained in itself, thereby improving the security of the password configured by the user and helping to guard against password cracking.

The password dictionary detection function detects a user-input password based on the following aspects:

- Detects a system-defaulted password dictionary: If the user-input password exists in the system-defaulted password dictionary, the user-configured password fails to pass the detection and the system displays a prompt indicating that the user cannot use this password.
- Detects a date dictionary, which is a birthday dictionary in most cases: The system detects a combination of four to eight digits for the user-input password, because the birthday password format is 4-digit mmdd, 5-digit yymmd or yymdd, 6-digit yymmdd or

yyyymd, 7-digit yyyymdd or yyyymmd, or 8-digit yyyymmdd, where the year yy ranges from 00 to 99, the year yyyy ranges from 1900 to 2100, the month mm ranges from 1 to 12, and the day dd ranges from 1 to 31.

- Detects a surname spelling dictionary: The system checks the user-input password against the spellings of the latest 100 common surnames.
- Detects a combination of the date dictionary and the name spelling dictionary: The system checks the user-input password against a combination of the date dictionary and the name spelling dictionary, which can be the combination of a birthday and a surname, the combination of a surname and a birthday, or a birthday or surname only.

Password Life Cycle

The password life cycle defines the validity time of a user password. When the service time of a password exceeds the life cycle, the user needs to change the password.

If the user inputs a password that has already expired during login, the system will give a prompt, indicating that the password has expired and the user needs to reset the password. If the new password input during password resetting does not meet system requirements or the new passwords consecutively input twice are not the same, the system will ask the user to input the new password once again.

Guard Against Repeated Use of Passwords

When changing the password, the user will set a new password while the old password will be recorded as the user's history records. If the new password input by the user has been used previously, the system gives an error prompt and asks the user to specify another password.

The maximum number of password history records per user can be configured. When the number of password history records of a user is greater than the maximum number configured for this user, the new password history record will overwrite the user's oldest password history record.

Storage of Encrypted Passwords

Administrators can enable the storage of encrypted passwords for security consideration. When administrators run the **show running-config** command to display configuration or run the **write** command to save configuration files, various user-set passwords are displayed in the cipher text format. If administrators disable the storage of encrypted passwords next time, the passwords already in cipher text format will not be restored to plaintext passwords.

4.3 Configuration

Configuration	Description and Command	
Configuring the Password Security Policy	Optional configuration, which is used to configure a combination of parameters related to the password security policy.	
	password policy enable-secret-dictionary [birthday-only | name-only | both-birthday-name]	Configures the password dictionary detection function.
	password policy life-cycle	Configures the password life cycle.

	password policy min-size	Configures the minimum length of user passwords.
	password policy no-repeat-times	Sets the no-repeat times of latest password configuration, so that the passwords specified in these times of latest password configuration can no longer be used in future password configuration.
	password policy secret-dictionary weak *password*	Configures a user-defined weak password.
	password policy strong	Enables the strong password detection function.
	service password-encryption	Sets the storage of encrypted passwords.

Networking Requirements

- Provide a password security policy for local authentication of the device. Users can configure different password security policies to implement password security management.

Notes

- The configured password security policy is valid for global passwords (configured using the commands enable password and enable secret) and local user passwords (configured using the username name password password command). It is invalid for passwords in Line mode.

Configuration Steps

Configuring the Password Life Cycle

- Optional
- Perform this configuration on each device that requires the configuration of a password life cycle unless otherwise stated.

Configuring the Minimum Length of User Passwords

- Optional
- Perform this configuration on each device that requires a limit on the minimum length of user passwords unless otherwise stated.

Setting the No-Repeat Times of Latest Password Configuration

- Optional
- Perform this configuration on each device that requires a limit on the no-repeat times of latest password configuration unless otherwise stated.

Setting the Storage of Encrypted Passwords

- Optional
- Perform this configuration on each device that requires the storage of passwords in encrypted format unless otherwise stated.

Verification

Configure a local user on the device, and configure a valid password and an invalid password for the user.

- When you configure the valid password, the device correctly adds the password.
- When you configure the invalid password, the device displays a corresponding error log.

Related Commands

Configuring the Password Life Cycle

Command Syntax	**password policy life-cycle** *days*
Parameter Description	**life-cycle** *days*: Indicates the password life cycle in the unit of days. The value range is from 1 to 65535.
Command Mode	Global configuration mode
Usage Guide	The password life cycle is used to define the validity period of user passwords. If the user logs in with a password whose service time already exceeds the life cycle, a prompt is given, asking the user to change the password.

Configuring the Minimum Length of User Passwords

Command Syntax	**password policy min-size** *length*
Parameter Description	**min-size** *length*: Indicates the minimum length of passwords. The value range is from 1 to 31.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the minimum length of passwords. If the minimum length of passwords is not configured, users can input a password of any length.

Setting the No-Repeat Times of Latest Password Configuration

Command Syntax	**password policy no-repeat-times** *times*
Parameter Description	**no-repeat-times** *times*: Indicates the no-repeat times of latest password configuration. The value range is from 1 to 31.
Command Mode	Global configuration mode
Usage Guide	After this function is enabled, all old passwords used in the several times of latest password configuration will be recorded as the user's password history records. If the new password input by the user has been used previously, the system gives an error prompt and the password modification fails. You can configure the maximum number of password history records per user. When the number of password history records of a user is greater than the maximum number configured for the user, the new password history record will overwrite the user's oldest password history record.

Enabling the Strong Password Detection Function

Command Syntax	**password policy strong**
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	After the strong password detection function is enabled, a prompt is displayed for the following types of passwords: 1. Passwords that are the same as corresponding accounts; 2. Simple passwords that contain characters or digits only.

Setting the Storage of Encrypted Passwords

Command Syntax	**service password-encryption**
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	Before the storage of encrypted passwords is set, all passwords used in the configuration process will be displayed and stored in plaintext format, unless the passwords are configured in cipher text format. You can enable the storage of encrypted passwords for security consideration. When you run the **show running-config** command to display configuration or run the **write** command to save configuration files, various user-set passwords are displayed in the cipher text format. If you disable the storage of encrypted passwords next time, the passwords already in cipher text format will not be restored to plaintext passwords.

Checking User-Configured Password Security Policy Information

Command Syntax	**show password policy**
Parameter Description	-
Command Mode	Privileged EXEC mode/ Global configuration mode/ Interface configuration mode
Usage Guide	Use this command to display the password security policy configured on the device.

4.4 Monitoring

Displaying

Command	Function

show password policy	Displays user-configured password security policy information.

5 Configuring Software Authorization Management

5.1 Overview

Software authorization is an intermediate link for users to use some extension functions of the device. A user can use the extension functions after installing correct license files. The extension functions provided by FSOS include the number of users supported by the AP. A user can use general functions and extension functions of the FSOS after being authorized.

Generally, all features of the FSOS are installed for the device before delivery of the device. However, users cannot use some features of the FSOS before they obtain a corresponding license file.

Whether a feature requires authorization and the authorization type are specified in the configuration guide of the feature. Unless otherwise specified, basic functions of the system can be used without authorization.

5.2 Function Details

Basic Concept

License File for a Feature

A license for a certain special feature obtained by means of license file, hardware entity, or legal contract. This license stipulates the maximum number of users allowed to use it, the maximum number of instances allowed to be used, and validity period.

Authorized Software

Software function that can be used after being authorized.

Host Number

Unique serial number for identifying each device.

In VSU environment, a license can adopt the host ID of any chassis. When the chassis exits the VSU environment, the feature corresponding to the license becomes invalid.

Authorization by Products

One license file is applied to only one device, which matches the host number. License file migration is not supported.

Purchase Voucher

Purchase voucher of a license file. This voucher contains the product activation key (PAK) and the website for downloading the license file.

Product Activation Key (PAK)

The legal owner of the purchase voucher logs in to the website (listed on the purchase voucher) for downloading the license file and uses the PAK for registration. After that, a corresponding license file is provided on the webpage for downloading or directly sent to the registered mailbox.

License File

After a license file is installed on a device, users can use relevant functions. Each license file contains a digital signature to avoid manipulation. A license file is used for authorization based on products.

License Stacking

Different license files can be used on one device. For example, if a device provides both the FCoE and TRILL functions, users can purchase the license files of the two functions and use them on the same device.

Temporary License File

A temporary license file becomes invalid after a period of time.

Evaluation License File

Evaluation license file belongs to temporary license file. Generally, an evaluation license file is installed on a device before delivery, and it is mainly used to provide users with the function of using a certain trial feature. This type of license file is independent of the host number.

Permanent License File

A permanent license file is permanently valid.

Single-Instance License File

Only one license file can be installed for a feature at a time.

Multi-Instance License File

Multiple license files can be installed for the same feature on a device.

Currently, only the license file for the feature "number of users supported by the AP" is a multi-instance license file.

Friendly Period Warning

Friendly period warning is issued in log or TRAP form several days before the license file expires. Friendly period warning is set to prevent a license file with a validity period from stopping working suddenly when the validity period expires, ensuring network performance.

Functions and Features

Function and Feature	Description
Obtaining and Using a License File	Describe how to obtain and use a license file.
Backing Up, Updating, and Removing a License File	Describe how to back up, update, and remove a license file.

5.2.1 Obtaining and Using a License File

Using the License File

A license file must be purchased from the website or marketing channel of FSfor formal authorization. Authorization is based on each device. To obtain a license file, visit the website on the purchase voucher and provide the PAK and host ID. The license file can be directly

downloaded by a user or sent to a user by email. After obtaining the license file, users need to install the license file. After installing the license file, users can use the features corresponding to the license file.

The license files of the FSOS include permanent license file and temporary license file (evaluation license file is a type of temporary license file). Once a user starts using a temporary license for a certain feature, timekeeping is started for this license file, and this feature is disabled after the validity period of the license file expires. To continue using this feature, this user can purchase another license file (permanent or temporary license file) from the website or marketing channel of FS.

Check of the License File

After a device starts to run, the license file for each authorized feature needs to be checked. If the corresponding license file is properly installed, this feature is ready for application. Otherwise, this feature becomes invalid and cannot be used.

Checking the license files for various features occurs at different times. That is, the license files for some features are checked during startup, and the license files for some features are checked in real time.

Loss of the License File

License files are stored in the **data** directory of a device and will not be lost after software upgrade.

If the memory or file system is damaged with the license file backed up, you can install the backup license file again after system recovery. If the license file is not backed up, you can visit the authorization website of FSand obtain the license file again. The process of regaining the license file is the same as the process of obtaining a new license file (you do not need to purchase the license file again).

Authorization is based on each device. After a license file is provided for a specified device, authorization via this license file can be conducted on this device exclusively. The host ID may change during device maintenance or replacement. In case of host ID change, the license file obtained before can no longer be identified. In this case, contact the after-sales engineers of FS.

5.2.2 Backing Up, Updating, and Removing a License File

Backing Up a License File

In case that a fault such as file system storage media damage occurs on a device, the license file on this device may be lost after you rectify this fault. Therefore, you need to back up the license file for reinstallation in case of a fault.

Updating a License File

If the existing license file in the system cannot meet users' requirements for a feature, users can visit the website of FSto purchase a license file and then update the license file locally.

Removing a License File

If a feature is not needed, the user can remove the license file for this feature to improve the utilization rate of various resources like the memory. If the user want to use this feature again after removing its license file, t reinstall the license file. It is recommended that license files be kept properly.

5.3 Configuration Details

Configuration Item	Configuration Suggestion & Relevant Command	
Basic Functions of Software Authentication	Mandatory configuration. Installs a license file.	
	show license hostid	Obtains the host ID of the device.

	license install	Installs a license file manually.

5.3.1 Basic Functions of Software Authorization

Configuration Effect

A license file is installed to enable the corresponding function.

Notes

- After downloading a license file from a specified website, upload this license file to the device (or store it in a USB flash drive) for installation. You don't need to connect the device to the Internet during the installation.
- Different devices cannot share the same license file.
- After a license file is installed on a device, this license file is automatically backed up in the data directory of the system (the name of a license file ends with ".lic"). When you remove a license file, the backup file of this license file is also removed.

Configuration Steps

Obtaining Host ID of the Device

- Mandatory configuration.
- host-id indicates the host ID.
- If you want to apply a feature requiring authorization without installing the license file, the CLI displays a prompt indicating that the unauthorized feature is unavailable and provides the website for downloading the license file.

Command	**show license hostid**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	The name of a license file cannot be modified. This command does not require license.

Obtaining the PAK

- Mandatory configuration.
- Generally, a PAK is provided in a paper purchase voucher by FSafter a user purchases a license file.

Obtaining the License File of the Product from FSWeb URL

- Mandatory configuration.
- After logging in to the authorization website, you can obtain the license file according to the prompts.

Copying the License File to the File System of the Device

- Mandatory configuration.
- Use conventional file system operation commands to perform this operation. For example, download the license file through the TFTP protocol or copy the license file to a USB flash drive.

Installing the License File

- Optional. You can use the license-install or license auto-install command to install a license file. If you use the license install command in the VSU environment on the supervisor module, all devices in VSU are installed with the license file. For the non-supervisor module, only the device configured with the command is installed with the license file. If you use the license auto-install command in VSU environment, all devices are installed with the license file by auto-match. The two commands take the same effect in the non-VSU environment.

Command	**license install** { **flash: | usb0:** } *filename*
Parameter Description	**flash:** Specifies that the license file is installed in the internal flash file system. **usb0:** Specifies that the license file is installed in the USB file system. *filename*: Specifies the name of the license file.
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Verification

- You can run the show license all_license command to check the license name. If the license name is displayed, the corresponding license file is installed.

Command	**show license** { **all_license | file** [*license*] }
Parameter Description	**all_license**: Displays all license files already installed on the device. **file** *filename*: Displays a specified license file.
Command Mode	Privileged EXEC mode
Usage Guide	Users can check whether a license file is installed by checking the feature name.
Verification	N/A

Configuration Examples

Common Errors

- Install a license file that does not belong to the present device.
- No matching device is available.
- Reinstall a license file.
- Install a license file with its later version installed in the system..

5.3.2 Backing Up License File

Configuration Effect

- The license files of one or all features in the system are backed up.

Notes

- The license file of the evaluation version must not be backed up.
- License files can be backed up only when sufficient storage space is available.

Generally, one license file occupies a space ranging from 4 KB to 10 KB.

Configuration Steps

Backing Up a License File of the System

- The backup license file is a regular file.
- When you back up all license files in the system, a tar file is generated.

Command	**license** { **copy-all** | **copy-file** *filename* } { **flash:** | **usb0:** } [*target-filename*]
Parameter Description	**copy-all**: Copies all permanent license files in the system. **copy-file** *filename*: Copies the *filename* license file in the system. ***filename*** can be the name of a license file already installed in the system or the name of a feature. When ***filename*** is a feature name, all license files already installed for this feature are backed up. **flash:** Specifies that the license file is installed in the internal flash file system. **usb0:** Specifies that the license file is installed in the USB file system. *filename*: Specifies the name of the license file.
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Uploading a License File to Another System for Storage

- You can use a file system management command to further save a license file to other storage devices, such as a USB flash drive.

Verification

- You can run the dir command to check whether the license file backup is generated. In addition, you can check whether the backup is correct by comparing the output of the dir command with the license file name in the installed license field of the feature with permanent authorization displayed by running the show license all-license command.

Command	**dir** [*filesystem:*] [*file-url*]
Parameter Description	*filesystem*: The file system URL followed by a colon. The file systems include **flash:**, **sata:**, **usb:**, and **tmp:**. *file-url*: Path name. The path starting with "/" indicates an absolute path. Otherwise, it is a relative path.
Command Mode	Privileged EXEC mode
Usage Guide	This command does not require license.
Verification	FS#dir usb0:fs-license-lics Directory of usb0:/fs-license-lics 1 drwx 4096 Fri Jun 20 12:29:32 2014 . 2 drwx 4096 Fri Jun 20 12:28:37 2014 .. 3 -rwx 8704 Fri Jun 20 12:29:12 2014 lics.tar 1 file, 2 directories 536870912 bytes total (740,687,872 bytes free)

Command	**show license** { **all-license** | **file** [*license*] }
Parameter Description	**all-license**: Displays all license files already installed on the device. **file** *filename*: Displays a specified license file.
Command Mode	Privileged EXEC mode
Usage Guide	Users can check whether a license file is installed by checking the feature name. Only a multi-instance license file has the **installed license** field. The multi-instance license file backup is named after the ID of the multi-instance license file. At most one single-instance license file exists in the system at a time; therefore, the single-instance license file backup is named after the feature.

Verification	FS#show license all-license Searching license in the system... 1. Service name: LIC-AP-64 Attribute: Permanent, Multiple_instance, Releasable [Installed licenses] [Licensed serial number] 19881021.lic LIC-AP-6400000012264966 19881023.lic LIC-AP-6400000012264988

Configuration Examples

Backing Up All License Files of the System

Network Environment	Back up all license files in the system and name the backup lics.tar.
Configuration Steps	● Connect a USB flash drive to the device. ● Back up all permanent license files in the USB flash drive and name the backup lics.tar.
	FS#lic copy-all usb0:fs-license-lics/lics.tar Success to copy all permanent license.
Verification	● You can run the **dir** command to check whether the license file package is generated. After decompressing the package, you can check whether the backup is correct by comparing the files in the package with the license file name displayed in the **installed license** field of the feature with permanent authorization displayed by running the **show license all-license** command. Only a multi-instance license file has the **installed license** field. The multi-instance license file backup is named after the ID of the multi-instance license file. At most one single-instance license file exists in the system at a time; therefore, the internal single-instance license file backup is named after the feature. In this example, the IDs 19881021.lic and 19881023.lic are embedded in the license file. License files are stored in different folders based on the features during the packing; therefore, users can still identify the mapping between license files and features.
	FS#dir usb0:fs-license-lics Directory of usb0:/fs-license-lics 1 drwx 4096 Fri Jun 20 12:29:32 2014 . 2 drwx 4096 Fri Jun 20 12:28:37 2014 .. 3 -rwx 8704 Fri Jun 20 12:29:12 2014 lics.tar 1 file, 2 directories

	536870912 bytes total (740,687,872 bytes free) FS#show license all-license Searching license in the system... 1. Service name: LIC-AP-64 Attribute: Permanent, Multiple_instance, Releasable [Installed licenses] [Licensed serial number] 19881021.lic LIC-AP-6400000012264966 19881023.lic LIC-AP-6400000012264988

Common Errors

- Specify a license file or a file not in the system.
- Specify a temporary license file for backup (a temporary license file cannot be backed up).

5.3.3 Friendly Period Warning

Configuration Effect

- Before the validity period of an evaluation license file expires, a warning is issued in log mode, enabling users to take measures in advance.

Notes

- Each authorized feature should be set separately.
- This setting may be affected by device time adjustment.
- A permanent license file does not need to be configured with friendly period warning.

Configuration Steps

Configuring a Friendly Period Warning for an Authorized Feature

Command	**license grace-peroid** *filename days*
Parameter Description	*filename*: name of the license file for a feature *days*: The period from the expiry time to the warning time,
Defaults	The default value is the smaller one between 120 and half the evaluation license file's validity period.
Command Mode	Privileged EXEC mode
Usage Guide	-

Verification

- 1: Set the expiry time of a license file to be earlier than the warning time, and the warning is displayed at regular intervals.
- 2: Run the show license command to check whether the time of the Alarm starting point filed is consistent with the setting.

Command	**show license** { **all-license** | **file** [*license*] }
Parameter Description	**all-license**: Displays all license files already installed on the device. **file** *filename*: Displays a specified license file.
Command Mode	Privileged EXEC mode
Usage Guide	This command does not require license.
Verification	

Common Errors

- Set friendly period warning for a permanent license file.
- No license file is installed in the preset feature system.

5.3.4 Updating License File

Configuration Effect

- The license file for a feature of the system is updated. Generally, this configuration is performed to update an evaluation license file into a temporary license file.

Notes

- A formal permanent license file does not need to be updated.
- A license file cannot be updated to the earlier version.

A license file has a time filed. The value of this field is subject to the time when the license file is generated from the website. The later the time, the later the version.

Configuration Steps

Updating a License File

- You can run the license update command to update the license file for a feature.
- Update the license file without connecting the device to the Internet.

Command	**license update** { **flash:** | **usb0:** } *filename*
Parameter	**flash:** Specifies that the license file is installed in the internal flash file system.

Description	**usb0:** Specifies that the license file is installed in the USB file system. *filename*: Specifies the name of the license file.
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Verification

- You can run the show license command and check the Attribute field. If the field is displayed as Permanent, the corresponding attribute is updated.

Command	**show license** { **all-license** | **file** [*license*] }
Parameter Description	**all-license**: Displays all license files already installed on the device. **file** *filename*: Displays a specified license file.
Command Mode	Privileged EXEC mode
Usage Guide	This command does not require license.
Verification	

Configuration Examples

Common Errors

5.3.5 Removing License File

Configuration Effect

- Remove the license files for one or all features in the system.

If a feature is not needed, the user can remove the license file for this feature to improve the utilization rate of various resources like the memory. After being removed, this feature becomes unavailable.

Notes

- If you remove the license file in use, the removal operation takes effect next time when the feature is enabled or restarted.
- To reinstall a license file after removing it, you need to obtain the license file. It is recommended that you back up the license file before removing it.

Configuration Steps

Removing a License File from the System

- Run the license uninstall command to remove a license file from the system.

Command	**license uninstall** { **all** | *license [filename]* }
Parameter Description	**all**: Remove all license files in the system. *license*: name of the license file to be removed *filename*: name of the file to be removed
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	After you remove the license file for a feature that is running, the license file removal does not take effect immediately. A license file cannot be restored after it is removed. It is recommended that you back up the license file before removing it. This command does not require license.

Verification

- You can run the show license all-license command to display the Service name filed. If the name of a feature corresponding to a license file already removed is not displayed, the removal is successful.

Command	**show license** { **all-license** | **file** [*license*] }
Parameter Description	**all-license**: Displays all license files already installed on the device. **file** *filename*: Displays a specified license file.
Command Mode	Privileged EXEC mode
Usage Guide	This command does not require license.
Verification	FS#show license all-license Searching license in the system... 1. Service name: LIC-FCoE Attribute: Permanent, Single_instance, Releasable Licensed serial number: LIC-FCOE00000012268889

6 Configuring PKG_MGMT

6.1 Overview

Package management (pkg_mgmt) is a package management and upgrade module. This module is responsible for installing, upgrading/degrading, querying and maintaining various components of the device, among which upgrade is the main function. Through upgrade, users can install new version of software that is more stable or powerful. Adopting a modular structure, the FSOS system not only supports overall upgrade and subsystem upgrade but also supports separate upgrade of a feature package. In addition, the FSOS system supports upgrade through hot patches.

Component upgrade described in this document applies to both the box-type device. In addition, this document is for only version 11.0 and later, excluding those upgraded from earlier versions.

Protocols and Standards

N/A

6.2 Applications

Application	Scenario
Upgrading/Degrading Subsystem	Upgrade subsystem firmware like boot, kernel, and rootfs on the box-type device.
Upgrading/Degrading a Single Feature Package	Upgrade a single feature package on the box-type device.
Installing a Hot Patch Package	Install a hot patch, and repair a certain part of the feature component.

6.2.1 Upgrading/Degrading Subsystem

Scenario

After the upgrade of a subsystem firmware is complete, all system software on the device is updated, and the overall software is enhanced. Generally, the subsystem firmware of the box-type device is called main package.

The main features of this upgrade mode are as follows: All software on the device is updated after the upgrade is completed; all known software bugs are fixed. It takes a long time to finish upgrade.

Deployment

You can store the main package in the root directory of the TFTP server, download the package to the device, and then run an upgrade command to upgrade the package locally. You can also store the main package in a USB flash drive or SD card, connect the USB flash drive to the device, and then run an upgrade command to upgrade the package.

6.2.2 Upgrading Subsystem by One-click

Scenario

Upgrade the firmware automatically without interrupting services on a dual-device VSU system. While either in VSU mode or in standalone mode, one single device will restart after this configuration, thus interrupting services.

Deployment

You can store the main package in the root directory of the TFTP server, download the package to the device, and then run an upgrade command to upgrade the package locally. You can also store the main package in a USB flash drive or SD card, connect the USB flash drive or SD card to the device, and then run an upgrade command to upgrade the package.

6.2.3 Upgrading/Degrading a Single Feature Package

Scenario

Device software consists of several components, and each component is an independent feature module. After an independent feature package is upgraded, only the feature bug corresponding to this package is fixed. Besides, this feature is enhanced with the other features unchanged.

The features of this upgrade mode are as follows: Generally, a feature package is small and the upgrade speed is high. After the upgrade is completed, only the corresponding functional module is improved, and other functional modules remain unchanged.

Deployment

You can store this package in the root directory of the TFTP server, download the package to the local device, and then complete the upgrade. You can also store the package in a USB flash drive or SD card, connect the USB flash drive to the device, and then complete the upgrade.

6.2.4 Installing a Hot Patch Package

Scenario

To fix software bugs without restarting the device, you can install hot patch packages. Hot patch packages are only applicable to fixing a specific software version. Generally, hot patch packages are released to fix the software of a certain version only when the device cannot be started in the user's environment.

The most significant feature of hot patch upgrade is that all bugs can be fixed without device restart after the upgrade is completed.

Deployment

You can store this package in the root directory of the TFTP server, download the package to the local device, and then complete the upgrade. You can also store the package in a USB flash drive, connect the USB flash drive to the device, and then complete the upgrade.

6.3 1.3 Features

Basic Concepts

↘ Subsystem

A subsystem exists on a device in the form of images. The subsystems of the FSOS include:

- boot: After being powered on, the device loads and runs the boot subsystem first. This subsystem is responsible for initializing the device, and loading and running system images.
- kernel: kernel is the OS core part of the system. This subsystem shields hardware composition of the system and provides applications with abstract running environment.
- rootfs: rootfs is the collection of applications in the system.

Main Package and Rack Package

- Main package is often used to upgrade/degrade a subsystem of the box-type device. The main package is a combination package of the boot, kernel, and rootfs subsystems. The main package can be used for overall system upgrade/degradation.

Feature Package of FSOS

- The feature package of FSOS refers to a collection which enables a certain feature. When the device is delivered, all supported functions are contained in the rootfs subsystem. You can upgrade only a specific feature by upgrading a single feature package.

Hot Patch Package

- A hot patch package contains the hot patches of several features. You can upgrade a hot patch package to install patches for various features. New features are provided immediately without device restart after the upgrade.

"Firmware" in this document refers to an installation file that contains a subsystem or feature module.

Overview

Feature	Description
Upgrading/Degrading and Managing Subsystem Components	Upgrades/degrades a subsystem.
Upgrading/Degrading and Managing Functional Components	Upgrades/degrades a functional component.
Upgrading/Degrading and Managing Hot Patch Packages	Installs a hot patch package.

6.3.1 Upgrading/Degrading and Managing Subsystem Components

Subsystem upgrade/degradation aims to upgrade the software by replacing the subsystem components of the device with the subsystem components in the firmware. The subsystem component contains redundancy design. Subsystems of the device are not directly replaced with the subsystems in the package during upgrade/degradation in most cases. Instead, subsystems are added to the device and then activated during upgrade/degradation.

Working Principle

Upgrade/Degradation

Various subsystems exist on the device in different forms. Therefore, upgrade/degradation varies with different subsystems.

- boot: Generally, this subsystem exists on the norflash device in the form of images. Therefore, upgrading/degrading this subsystem is to write the image into the norflash device.
- kernel: This subsystem exists in a specific partition in the form of files. Therefore, upgrading/degrading this subsystem is to write the file.
- rootfs: Generally, this subsystem exists on the nandflash device in the form of images. Therefore, upgrading/degrading this subsystem is to write the image into the nandflash device.

Management

Query the subsystem components that are available currently and then load subsystem components as required.

Each subsystem component contains redundancy design. During the upgrade/degradation:

- boot: The boot subsystem always contains a master boot subsystem and a slave boot subsystem. Only the master boot subsystem is involved in the upgrade, and the slave boot subsystem serves as the redundancy backup all along.
- kernel: as the kernel subsystem contains at least one redundancy backup. More redundancy backups are allowed if there is enough space.
- rootfs: The rootfs subsystem always contains a redundancy backup.

The boot component is not included in the scope of subsystem management due to its particularity. During upgrade of the kernel or rootfs subsystem component, the upgrade/degradation module always records the subsystem component in use, the redundant subsystem component, and management information about various versions.

Relevant Configuration

Upgrade

- Store the upgrade file on the local device, and then run the upgrade command for upgrade.

6.3.2 Upgrading/Degrading and Managing Functional Components

Working Principle

In fact, upgrading a feature is replacing feature files on the device with the feature files in the package.

Managing feature components and hot patches is aimed at recording the information of feature components and hot patches by using a database. In fact, installing, displaying and uninstalling a component is the result of performing the Add, Query and Delete operation on the database.

After package upgrade, component upgrade cannot be performed.

Relevant Configuration

Upgrade

- Store the upgrade file on the local device, and then run the upgrade command for upgrade.

6.3.3 Upgrading/Degrading and Managing Hot Patch Packages

Working Principle

In fact, upgrading a feature component is replacing feature files on the device with the feature files in the package.

Upgrading hot patch packages is similar to upgrading features. The difference is that only files to be revised are replaced during hot patch package upgrade. In addition, after the files are replaced, the new files take effect automatically.

After package upgrade, component upgrade cannot be performed.

Management

Similar to feature component management, hot patch management also includes the query, installation, and uninstallation operation, which is the result of adding, querying and deleting data respectively.

Hot patches and feature components are managed based on the same technology. The difference is that the hot patches involve three different states, that is, Not installed, Installed, and Activated. These states are described as follows:

The hot patch in Installed state only indicates that this hot patch exists on the device, but it has not taken effect yet.

Only the hot patch in Activated state is valid.

Relevant Configuration

Upgrade

- Store the upgrade file in the local file system, and then run the upgrade command for upgrade.

Activating a Hot Patch

- You can run the patch active command to activate a patch temporarily. The patch becomes invalid after device restart. To use this patch after device restart, you need to activate it again.
- You can also run the patch running command to activate a patch already permanently. The patch is still valid after device start.
- The patch not activated will never become valid.

Deactivating a Hot Patch

- To deactivate an activated patch, run the patch deactive command.

Uninstalling a Hot Patch

- You can run the patch delete command to uninstall a hot patch.

6.4 Configuration

Configuration	Description and Command	
Upgrading/Degrading a Firmware	The basic function of the configuration is installing and upgrading/degrading a subsystem firmware, feature package, and hot patch package.	
	upgrade *url* [**force**]	*url* is a local path where the firmware is stored. This command is used to upgrade the firmware stored on the device.
	upgrade download tftp:/ *path* [**force**]	*path* is the path of the firmware on the server. This command is used to download a firmware from the server and upgrade the package automatically.
	upgrade download oob_tftp://*path* [**force**]	*path* is the path of the firmware on the server. **via mgmt** *number*: If the transfer mode is *oob_tftp* and there are multiple MGMT ports, you can select a specific port. This command is used to download a firmware from the server and upgrade the package automatically.
	upgrade rollback	Rolls back subsystem firmware.
	patch active	Activates a patch temporarily.

	patch running	Activates a patch permanently,
Deactivating and Uninstalling a Hot Patch	(Optional) Deactivates or uninstalls a hot patch.	
	upgrade deactive	Deactivates an activated patch.
	patch delete	Uninstalls a hot patch.

6.4.1 Upgrading/Degrading a Firmware

Configuration Effect

Available firmwares include the main package, rack package, various feature packages and hot patch packages.

- After the upgrade of the main package is complete, all system software on the line card is updated, and the overall software is enhanced.
- After an independent feature package is upgraded, only the feature bug corresponding to this package is fixed. Besides, this feature is enhanced, with other features remain unchanged.
- Upgrading hot patch packages is aimed at fixing software bugs without restarting the device. Hot patch packages are only applicable to fixing bugs for a specific version of software.

Generally a main package is released to upgrade a box-type device.

Notes

N/A

Configuration Steps

Upgrading the Main Package for a Single Device

- Optional configuration. This configuration is required when all system software on the device needs to be upgraded.
- Download the firmware to the local device and run the upgrade command.

Generally a main package is pushed to upgrade a box-type device.

Upgrading a Main Package on a VSU

- Optional configuration. This configuration is required when all system software on a VSU needs to be upgraded without service interruption.
- Download the firmware to the local device and run the upgrade auto command.

Upgrading Each Feature Package

- Optional configuration. The configuration is used to fix bugs of a certain feature and enhance the function of this feature.
- Download the firmware to the local device and run the upgrade command.

Upgrading a Hot Patch Package

- Optional configuration. The configuration is used to fix software bugs without restarting the device.
- Download the firmware to the local device and run the upgrade command.

- After being upgraded, the hot patch can be used after it is activated. The configuration in this step is mandatory. Two activation modes are available: Run the patch active command to activate a patch temporarily, or run the patch running command to activate a patch permanently.

Generally, the **patch running** command must be used to activate a patch permanently in the user scenario. The **patch active** command can be used to activate a patch only when a user intends to verify the patch.

Subsystem Rollback

- Optional configuration. This configuration aims to roll a subsystem back to the state before the upgrade, select this configuration item..
- This configuration takes effect after you run the upgrade command to upgrade the subsystem component (for example, the main package).

After you run the **upgrade** command to upgrade a subsystem component in the user scenario, you can run the rollback command once, that is, consecutive rollback is not supported.

Verification

- After upgrading a subsystem component, you can run the show upgrade history command to check whether the upgrade is successful.
- After upgrading a feature component, you can run the show component command to check whether the upgrade is successful.
- After upgrading a hot patch package, you can run the show patch command to check whether the upgrade is successful.

Commands

Upgrade

Command	**upgrade** *url* [**force**]
Parameter Description	**force**: indicates forced upgrade.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Command	**upgrade download tftp:/***path* [**force**] **upgrade download oob_tftp:/***path* [**force**]
Parameter Description	**force** indicates forced upgrade.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying the Firmware Stored on the Device

Command	**show upgrade file** *url*

Parameter Description	*url* indicates the path of the firmware in the device file system.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying Upgrade History

Command	**show upgrade history**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Subsystem Component Rollback

Command	**upgrade rollback**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to undo the last subsystem upgrade operation and make the subsystem restore to the state before the upgrade. You can perform the rollback operation only if the last upgrade is subsystem upgrade and the upgrade is successful. The rollback command cannot be executed in succession.

Displaying the Feature Components Already Installed

Command	**show component**
Parameter Description	[*component_name*]: component name When this parameter value is N/A, the command is used to display all components already installed on the device and basic information of these components. When this parameter value is not N/A, the command is used to display detailed information of the corresponding component, check whether the component is intact, and check whether this component works properly.
Command Mode	Privileged EXEC mode
Usage Guide	

Displaying the Patch Packages Already Installed

Command	**show patch**
Parameter	N/A

Description	
Command Mode	Privileged EXEC mode
Usage Guide	

Activating the Patches Temporarily

Command	**patch active**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	This operation can be performed only on the device already installed with a patch. This command can be used to activate a patch temporarily, and the activated patch becomes invalid after device restart.

Activating the Patches Permanently

Command	**patch running**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	This operation can be performed only on the device already installed with a patch. This command can be used to activate a patch permanently.

Configuration Example

Example of Upgrading a Subsystem Firmware on the Box-Type Device

Network Environment	Before the upgrade, you must copy the firmware to the device. The upgrade module provides the following solutions. ● Run some file system commands like **copy tftp** and **copy xmodem** to copy the firmware on the server to the device file system, and then run the **upgrade** *url* command to upgrade the firmware in the local file system. ● Run the **upgrade download tftp://***path* command directly to upgrade the firmware file stored on the tftp server. ● Copy the firmware to a USB flash drive, insert the USB flash drive to the device, and then run the **upgrade** *url* command to upgrade the firmware in the USB flash drive.
Configuration Steps	● Run the upgrade command. ● After upgrading the subsystem, restart the device.
Verification	● Check the system version on the current device. If the version information changes, the upgrade is successful.

Example of Upgrading a Feature Package on the Box-Type Device

Network Environment	Before the upgrade, you must copy the firmware to the device. The upgrade module provides the following solutions. ● Run some file system commands like **copy tftp** and **copy xmodem** to copy the firmware on the server to the device file system, and then run the **upgrade** *url* command to upgrade the firmware in the local file system. ● Run the **upgrade download tftp://***path* command directly to upgrade the firmware file stored on the tftp server. ● Copy the firmware to a USB flash drive, connect the USB flash drive to the device, and then run the **upgrade** *url* command to upgrade the firmware in the USB flash drive.
	●
Configuration Steps	● Run the **upgrade** command. ● Check whether the device needs to be restarted based on the prompt displayed after the upgrade.
Verification	● Check the version of the feature component on the current device. If the version information changes, the upgrade is successful.
	FS# show component Package :sysmonit Version:1.0.1.23cd34aa Build time: Wed Dec 7 00:58:56 2011 Size:12877 Install time :Wed Mar 5 14:23:12 2012 Description:this is a system monit package Required packages: None ---------- package:bridge Version: 2.3.1.1252ea Build time: Wed Dec 7 00:54:56 2011 Size:26945 Install time : Wed Mar 19:23:15 2012 Description:this is a bridge package Required packages: None

Example of Upgrading a Main Package for a VSU

Network Environment	Before the upgrade, you must copy the firmware to the device. The upgrade module provides the following solutions. 1 Run some file system commands like **copy tftp** and **copy xmodem** to copy the firmware on the server to the device file system, and then run the **upgrade auto** *url* command to upgrade the firmware in the local file system. 2 Copy the firmware to a USB flash drive, Insert the USB flash drive to the device, and then run the **upgrade auto** *url* command to upgrade the firmware in the USB flash drive.
Configuration	● Run the **upgrade auto** command.

Steps	● The VSU active and standby devices are restarted in sequence.

```
2015-04-09_09-56-23 FS#upgrade auto usb0:S6220_FSOS11.0(5)B1_install.bin
2015-04-09_09-56-24 FS#*Jan    1 00:23:40: %7:
2015-04-09_09-56-24 *Jan    1 00:23:40: %7: [Slot 1/0]:Upgrade processing is 10%
2015-04-09_09-56-26 FS#show upgrade status
2015-04-09_09-56-26 [Slot 1/0]
2015-04-09_09-56-26              dev_type: s6k
2015-04-09_09-56-26              status    : upgrading
2015-04-09_09-56-26 [Slot 2/0]
2015-04-09_09-56-26              dev_type: s6k
2015-04-09_09-56-26              status    : transmission
2015-04-09_09-58-20 *Jan    1 00:25:36: %7: [Slot 2/0]:Upgrade processing is 10%
2015-04-09_09-58-30 FS#show upgrade status
2015-04-09_09-58-30 [Slot 1/0]
2015-04-09_09-58-30              dev_type: s6k
2015-04-09_09-58-30              status    : upgrading
2015-04-09_09-58-30 [Slot 2/0]
2015-04-09_09-58-30              dev_type: s6k
2015-04-09_09-58-30              status    : upgrading
2015-04-09_09-58-39 *Jan    1 00:25:56: %7:
2015-04-09_09-58-39 *Jan    1 00:25:56: %7: [Slot 2/0]:Upgrade processing is 60%
2015-04-09_09-59-19 *Jan    1 00:26:35: %7:
2015-04-09_09-59-19 *Jan    1 00:26:35: %7: [Slot 2/0]:Upgrade processing is 90%
2015-04-09_09-59-19 *Jan    1 00:26:35: %7:
2015-04-09_09-59-19 *Jan    1 00:26:35: %7: [Slot 2/0]:
2015-04-09_09-59-19 *Jan    1 00:26:35: %7: Upgrade info [OK]
2015-04-09_09-59-19 *Jan    1 00:26:36: %7:      Kernel version[2.6.32.6b311610a8eb91->2.6.32.6b31161115502c]
2015-04-09_09-59-19 *Jan    1 00:26:36: %7:      Rootfs version[1.0.0.eb75cd01->1.0.0.3d978b6c]
2015-04-09_09-59-19 *Jan    1 00:26:36: %7:
2015-04-09_09-59-19 *Jan    1 00:26:36: %7: [Slot 2/0]:Reload system to take effect!
2015-04-09_09-59-21 *Jan    1 00:26:37: %7:
2015-04-09_09-59-21 *Jan    1 00:26:37: %7: [Slot 2/0]:Upgrade processing is 100%
2015-04-09_10-00-28 FS#show upgrade status
```

```
2015-04-09_10-00-28 [Slot 1/0]
2015-04-09_10-00-28          dev_type: s6k
2015-04-09_10-00-28          status    : upgrading
2015-04-09_10-00-28 [Slot 2/0]
2015-04-09_10-00-28          dev_type: s6k
2015-04-09_10-00-28          status    : success
2015-04-09_10-01-39 *Jan    1 00:28:56: %7:
2015-04-09_10-01-39 *Jan    1 00:28:56: %7: [Slot 1/0]:Upgrade processing is 60%
2015-04-09_10-02-17 *Jan    1 00:29:33: %7:
2015-04-09_10-02-17 *Jan    1 00:29:33: %7: [Slot 1/0]:Upgrade processing is 90%
2015-04-09_10-02-17 *Jan    1 00:29:33: %7:
2015-04-09_10-02-17 *Jan    1 00:29:33: %7: [Slot 1/0]:
2015-04-09_10-02-17 *Jan    1 00:29:34: %7: Upgrade info [OK]
2015-04-09_10-02-17 *Jan    1 00:29:34: %7:      Kernel version[2.6.32.6b311610a8eb91->2.6.32.6b31161115502c]
2015-04-09_10-02-17 *Jan    1 00:29:34: %7:      Rootfs version[1.0.0.eb75cd01->1.0.0.3d978b6c]
2015-04-09_10-02-17 *Jan    1 00:29:34: %7:
2015-04-09_10-02-18 *Jan    1 00:29:34: %7: [Slot 1/0]:Reload system to take effect!
2015-04-09_10-02-19 *Jan    1 00:29:35: %7:
2015-04-09_10-02-19 *Jan    1 00:29:35: %7: [Slot 1/0]:Upgrade processing is 100%
2015-04-09_10-02-19 *Jan    1 00:29:36: %7: %PKG_MGMT:auto-sync config synchronization, Please wait for a
moment....
2015-04-09_10-02-20 *Jan    1 00:29:36: %7:
2015-04-09_10-02-20 [ 1784.116069] rtc-pcf8563 6-0051: retrieved date/time is not valid.
2015-04-09_10-02-20 *Jan    1 00:29:36: %7: [Slot 2/0]:auto sync config: space not enough left 57229312, need
114597815
2015-04-09_10-02-20 *Jan    1 00:29:36: %7:
2015-04-09_10-02-20 *Jan    1 00:29:36: %7: [Slot 2/0]:auto sync package config err
2015-04-09_10-02-20 *Jan    1 00:29:37: %7: [Slot 1/0]
2015-04-09_10-02-21 *Jan    1 00:29:37: %7:      device_name: s6k
2015-04-09_10-02-21 *Jan    1 00:29:37: %7:      status:          SUCCESS
2015-04-09_10-02-21 *Jan    1 00:29:37: %7: [Slot 2/0]
2015-04-09_10-02-21 *Jan    1 00:29:37: %7:      device_name: s6k
2015-04-09_10-02-21 *Jan    1 00:29:37: %7:      status:          SUCCESS
2015-04-09_10-02-21 *Jan    1 00:29:38: %7: %Do with    dtm callback....
```

	2015-04-09_10-02-21 *Jan 1 00:29:38: %VSU-5-DTM_AUTO_UPGRADE: Upgrading the system, wait a moment please.
Verification	If the version information changes, the upgrade is successful.
	FS-VSU#show version detail System description : FSFull 10G Routing Switch(S6220-48XS4QXS-II) By FSNetworks System start time : 1970-02-07 00:33:24 System uptime : 0:00:47:28 System hardware version : 2.00 System software version : S6220_FSOS 11.0(5)B1 System patch number : NA System software number : M01181304092015 System serial number : 1234942570019 System boot version : 1.2.9.f23dcbe(150317) System core version : 2.6.32.6b31161115502c Module information: Slot 2/0 : S5860-48SC Hardware version : 2.00 System start time : 1970-02-07 00:33:24 Boot version : 1.2.9.f23dcbe(150317) Software version : S5860_FSOS 11.0(5)B1 Software number : M01181304092015 Serial number : 1234942570019 Slot 1/0 : S5860-48SC Hardware version : 2.00 System start time : 1970-02-07 00:33:47 Boot version : 1.2.9.f23dcbe(150317) Software version : S5860_FSOS 11.0(5)B1 Software number : M01181304092015 Serial number : 1234942570018

Example of Installing a Patch Package on the Box-Type Device

Network Environment	Before the upgrade, you must copy the firmware to the device. The upgrade module provides the following solutions. ● Run some file system commands like **copy tftp** and **copy xmodem** to copy the firmware on the server to the device file system, and then run the **upgrade** ***url*** command to upgrade the firmware in the local file system.

	● Run the **upgrade download tftp://*path*** command directly to upgrade the firmware file stored on the tftp server. ● Copy the firmware to a USB flash drive, connect the USB flash drive to the device, and then run the **upgrade *url*** command to upgrade the firmware in the USB flash drive.
Configuration Steps	● Run the upgrade command. ● Activate the hot patch.
Verification	● Check the hot patches installed on the current device.
	:patch package patch_install installed in the system, version:pa1 Package : patch_bridge Status: running Version: pa1 Build time: Mon May 13 09:03:07 2013 Size: 277 Install time: Tue May 21 03:07:17 2013 Description: a patch for bridge Required packages: None

Example of Subsystem Rollback on the Box-Type Device

You can perform the rollback operation only if the last upgrade is subsystem upgrade and the upgrade is successful. The rollback command cannot be executed in succession.

Network Environment	Before the upgrade, you must copy the firmware to the device. The upgrade module provides the following solutions. ● Run some file system commands like **copy tftp** and **copy xmodem** to copy the firmware on the server to the device file system, and then run the **upgrade *url*** command to upgrade the firmware in the local file system. ● Run the **upgrade download tftp://*path*** command directly to upgrade the firmware file stored on the tftp server. ● Copy the firmware to a USB flash drive, connect the USB flash drive to the device, and then run the **upgrade *url*** command to upgrade the firmware in the USB flash drive.
Configuration Steps	● Run the subsystem rollback command. ● Restart the device for the rollback to take effect.
	FS#upgrade rollback kernel rollback version[2.6.32.9f8b56f->2.6.32.91f9d21][OK] rootfs rollback version[1.0.0.1bcc12e8->1.0.0.2ad02537][OK] Rollback success! Reload system to take effect! Reload system?(Y/N)y Restarting system.
Verification	● Check the system version on the current device. If t it is restored to the version before the upgrade, the rollback is successful.

	FS#show upgrade history Last Upgrade Information: Time: 2014-08-31 12:15:03 Method: LOCAL Package Name: N18000_FSOS11.0(1)B1_CM_01200616_install.bin Package Type: Distribution

Common Errors

If an error occurs during the upgrade, the upgrade module displays an error message. The following provides an example:

```
Upgrade info [ERR]
        Reason:creat config file err(217)
```

The following describes several types of common error messages:

- Invalid firmware: The cause is that the firmware may be damaged or incorrect. It is recommended to obtain the firmware again and perform the upgrade operation.
- Firmware not supported by the device: The cause is that you may use the firmware of other devices by mistake. It is recommended to obtain the firmware again, verify the package, and perform the upgrade operation.

6.4.2 Deactivating and Uninstalling a Hot Patch

Configuration Effect

An activated hot patch is deactivated or uninstalled.

Notes

A hot patch that is not activated does not take effect; therefore, you cannot deactivate it.

Configuration Steps

Deactivating an Activated Patch

- Optional configuration. To deactivate an activated patch, run the patch deactive command.

Uninstalling a Hot Patch

- Optional configuration. To uninstall a hot patch already installed, run the **patch delete** command.

Verification

- You can run the show patch command to check whether a patch is activated or uninstalled.

Commands

Deactivating an Activated Patch

Command	**patch deactive**

Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	You can perform this operation on only an activated patch.

Deleting a Hot Patch

Command	**patch delete**
Parameter Description	
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to remove the hot patch package from the device.

Configuration Example

Deactivating and Uninstalling a Patch on the Box Device

Configuration Steps	● Run the patch deactivation command. ● Run the patch deletion command.
	FS#patch deactive Deactive the patch package success FS# patch delete Clear the patch patch_bridge success Clear the patch success
Verification	● Display patch status.
	FS#show patch No patch package installed in the system

Common Errors

- Run the patch deactive command when the patch is not activated. It is recommended to check the patch status. You can run the patch deactive command only when the patch is in the status:running state.

6.5 1.5 Monitoring

Clearing

Function	Command
Deletes a hot patch package already installed.	**patch delete**

Displaying

Function	Command
Displays all components already installed on the current device and their information.	**show component** [*component_name*]
Displays the information about the hot patch packages already installed on the device.	**show patch** [*patch_name*]
Displays the upgrade history.	**show upgrade history**

7 Configuring CWMP

7.1 Overview

CPE WAN Management Protocol (CWMP) provides a general framework of unified device management, related message specifications, management methods, and data models, so as to solve difficulties in unified management and maintenance of dispersed customer-premises equipment (CPEs), improve troubleshooting efficiency, and save O&M costs.

CWMP provides the following functions:

- Auto configuration and dynamic service provisioning. CWMP allows an Auto-Configuration Server (ACS) to automatically provision CPEs who initially access the network after start. The ACS can also dynamically re-configure running CPEs.
- Firmware management. CWMP manages and upgrades the firmware and its files of CPEs.
- Software module management. CWMP manages modular software according to data models implemented.
- Status and performance monitoring. CWMP enables CPEs to notify the ACE of its status and changes, achieving real-time status and performance monitoring.
- Diagnostics. The ACE diagnoses or resolves connectivity or service problems based on information from CPEs, and can also perform defined diagnosis tests.

Protocols and Standards

For details about TR069 protocol specifications, visit http://www.broadband-forum.org/technical/trlist.php.

Listed below are some major CWMP protocol specifications:

- TR-069_Amendment-4.pdf: CWMP standard
- TR-098_Amendment-2.pdf: Standard for Internet gateway device data model
- TR-106_Amendment-6.pdf: Standard for CPE data model
- TR-181_Issue-2_Amendment-5.pdf: Standard for CPE data model 2
- tr-098-1-4-full.xml: Definition of Internet gateway device data model
- tr-181-2-4-full.xml: Definition 2 of CPE data model 2

7.2 Applications

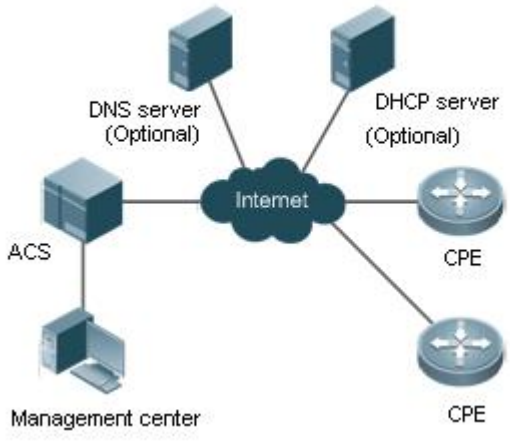
Typical Application	Scenario
CWMP Network Application Scenario	Initiate CPE-ACS connection, so as to upgrade the CPE firmware, upload the configuration files, restore the configuration, and realize other features.

7.2.1 CWMP Network Application Scenario

Application Scenario

The major components of a CWMP network architecture are CPEs, an ACS, a management center, a DHCP server, and a Domain Name System (DNS) server. The management center manages a population of CPEs by controlling the ACS on a Web browser.

Figure 7- 1



Note	● If the Uniform Resource Locator (URL) of the ACS is configured on CPEs, the DHCP server is optional. If not, the DHCP is required to dynamically discover the ACS URL. ● If the URLs of the ACS and CPEs contain IP addresses only, the DNS server is optional. If their URLs contain domain names, the DNS server is required to resolves the names.

Functional Deployment

HTTP runs on both CPEs and the ACS.

7.3 Features

Basic Concept

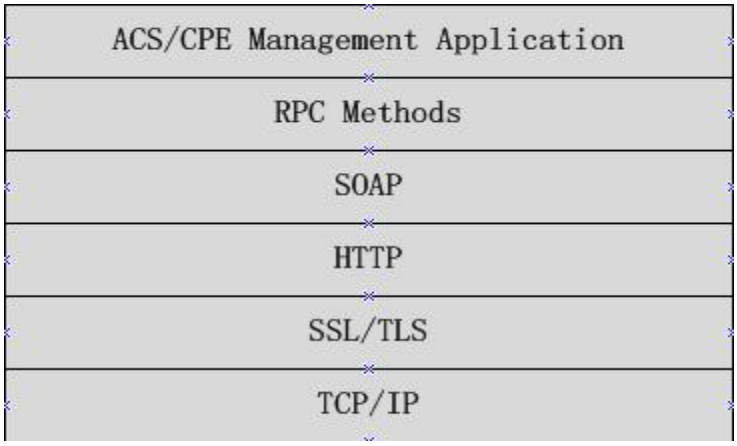
↘ Major Terminologies

- CPE: Customer Premises Equipment
- ACS: Auto-Configuration Server
- RPC: Remote Procedure Call
- DM: Data Model

↘ Protocol Stack

Figure 7- 2 shows the protocol stack of CWMP.

Figure 7- 2 CWMP Protocol Stack



As shown in Figure 7- 2, CWMP defines six layers with respective functions as follows:

- ACS/CPE Application

The application layer is not a part of CWMP. It is the development performed by various modules of the CPEs/ACS to support CWMP, just like the Simple Network Management Protocol (SNMP), which does not cover the MIB management of functional modules.

- RPC Methods

This layer provides various RPC methods for interactions between the ACS and the CPEs.

- SOAP

The Simple Object Access Protocol (SOAP) layer uses a XML-based syntax to encode and decode CWMP messages.. Thus, CWMP messages must comply with the XML-based syntax.

- HTTP

All CWMP messages are transmitted over Hypertext Transfer Protocol (HTTP). Both the ACS and the CPEs can behave in the role of HTTP clients and servers. The server function is used to monitor reverse connections from the peer.

- SSL/TLS

The Secure Sockets Layer (SSL) or Transport Layer Security (TLS) layer guarantees CWMP security, including data integrity, confidentiality, and authentication.

- TCP/IP

This layer is the (Transmission Control Protocol/Internet Protocol (TCP/IP) protocol stack.

↘ RPC Methods

The ACS manages and monitors CPEs by calling mostly the following RPC methods:

- Get RPC Methods

The Get methods enable the ACS to remotely obtain the set of RPC methods, as well as names, values and attributes of the DM parameters supported on CPEs.

- Set RPC Methods

The Set methods enable the ACS to remotely set the values and attributes of the DM parameters supported on CPEs.

- Inform RPC Methods

The Inform methods enable CPEs to inform the ACS of their device identifiers, parameter information, and events whenever sessions are established between them.

- Download RPC Methods

The Download method enables the ACS to remotely control the file download of CPEs, including firmware management, upgrade, and Web package upgrade.

- Upload RPC Methods

The Upload method enables the ACS to remotely control the file upload of CPEs, including upload of firmware and logs.

- Reboot RPC Methods

The Reboot method enables the ACS to remotely reboot the CPEs.

Session Management

CWMP sessions or interactions are the basis for CWMP. All CWMP interactions between the ACS and CPEs rely on their sessions. CWMP helps initiate and maintain ACS-CPE sessions to link them up for effective management and monitoring. An ACS-CPE session is a TCP connection, which starts from the Inform negotiation to TCP disconnection. The session is classified into CPE Initiated Session and ACS Initiated Session according to the session poster.

DM Management

CWMP operates based on CWMP Data Model (DM). CWMP manages all functional modules by a set of operations performed on DM. Each functional module registers and implements a respective data model, just like the MIBs implemented by various functional modules of SNMP.

A CWMP data model is represented in the form of a character string. For a clear hierarchy of the data model, a dot (.) is used as a delimiter to distinguish an upper-level data model node from a lower-level data model node. For instance, in the data model **InternetGatewayDevice.LANDevice**, **InternetGatewayDevice** is the parent data model node of **LANDevice**, and **LANDevice** is the child data model node of **InternetGatewayDevice**.

DM nodes are classified into two types: object nodes and parameter nodes. The parameter nodes are also known as leaf nodes. An object node is a node under which there are child nodes, and a parameter node is a leaf node under which there is no any child node. Object nodes are further classified into single-instance object nodes and multi-instance object nodes. A single-instance object node is an object node for which there is only one instance, whereas a multi-instance object node is an object node for which there are multiple instances.

DM nodes can also be classified into readable nodes and readable-and-writable nodes. A readable node is a node whose parameter values can be read but cannot be modified, and a readable-and-writable node is a node whose parameter values can be both read and modified.

A data model node has two attributes. One attribute relates to a notification function; that is, whether to inform the ACS of changes (other than changes caused by CWMP) to parameter values of the data model. The other attribute is an identifier indicating that the parameters of the data model node can be written using other management modes (than the ACS); that is, whether the values of the parameters can be modified using other management modes such as Telnet. The ACS can modify the attributes of the data models using RPC methods.

CWMP manages the data models using corresponding RPC methods.

Event Management

When some events concerned by the ACS occur on the CPE, the CPE will inform the ACS of these events. The ACS monitors these events to monitor the working status of the CPE. The CWMP events are just like Trap messages of SNMP or product logs. Using RPC methods, to

the ACS filters out the unconcerned types of events. CWMP events are classified into two types: single or (not cumulative) events and multiple (cumulative) events. A single event means that there is no quantitative change to the same event upon re-occurrence of the event, with the old discarded and the newest kept. A multiple event means that the old are not discarded and the newest event is kept as a complete event when an event re-occurs for multiple times later; that is, the number of this event is incremented by 1.

All events that occur on the CPE are notified to the ACS using the INFORM method.

Features

Feature	Description
Upgrading the Firmware	The ACS controls the upgrade of the firmware of a CPE using the Download method.
Upgrading the Configuration Files	The ACS controls the upgrade of the configuration files of a CPE using the Download method.
Uploading the Configuration Files	The ACS controls the upload of the configuration files of a CPE using the Upload method.
Backing up and Restoring a CPE	When a CPE breaks away from the management center, this feature can remotely restore the CPE to the previous status.

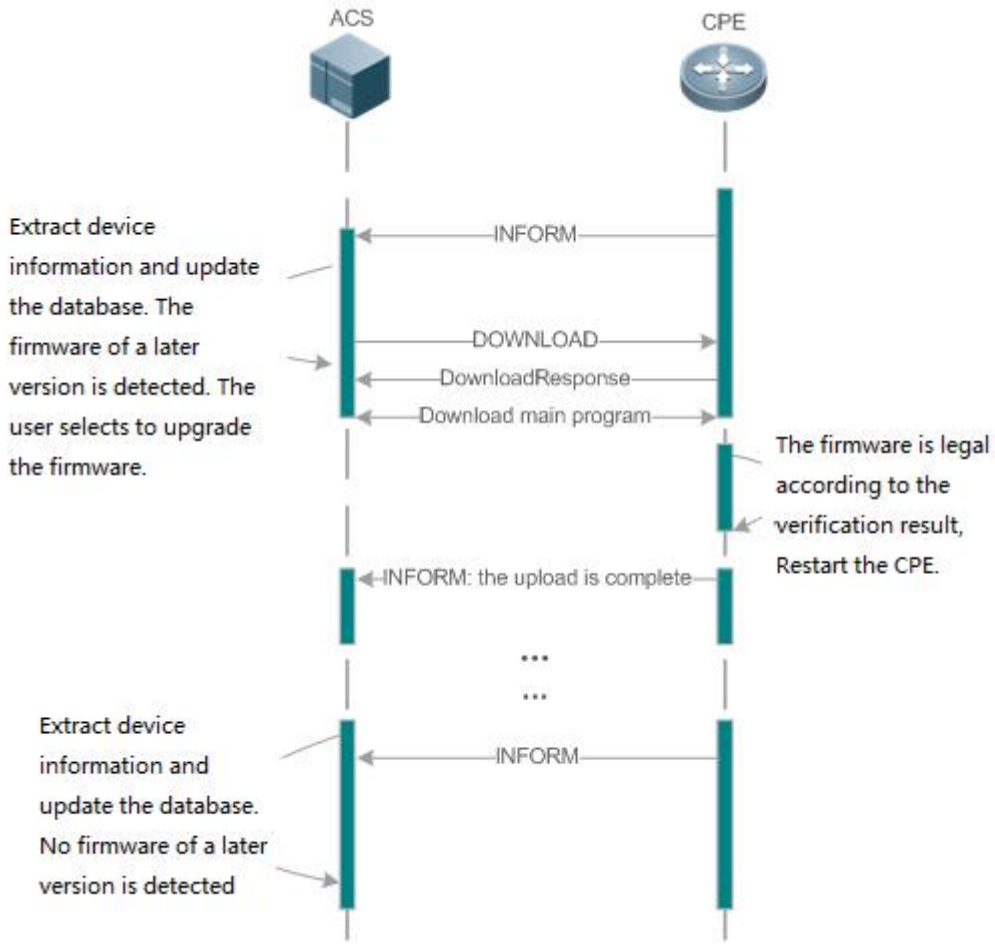
7.3.1 Upgrading the Firmware

Upgrading the Firmware means the firmware of a network element (NE) can be upgraded, so as to implement device version upgrade or replacement.

Working Principle

↘ **Sequence Diagram of Upgrading the Firmware**

Figure 7- 3



Users specify a CPE for the ACS to deliver the Download method for upgrading the firmware. The CPE receives the request and starts to download the latest firmware from the destination file server, upgrade the firmware, and then reboot. After restart, the CPE will indicate the successful or unsuccessful completion of the method application.

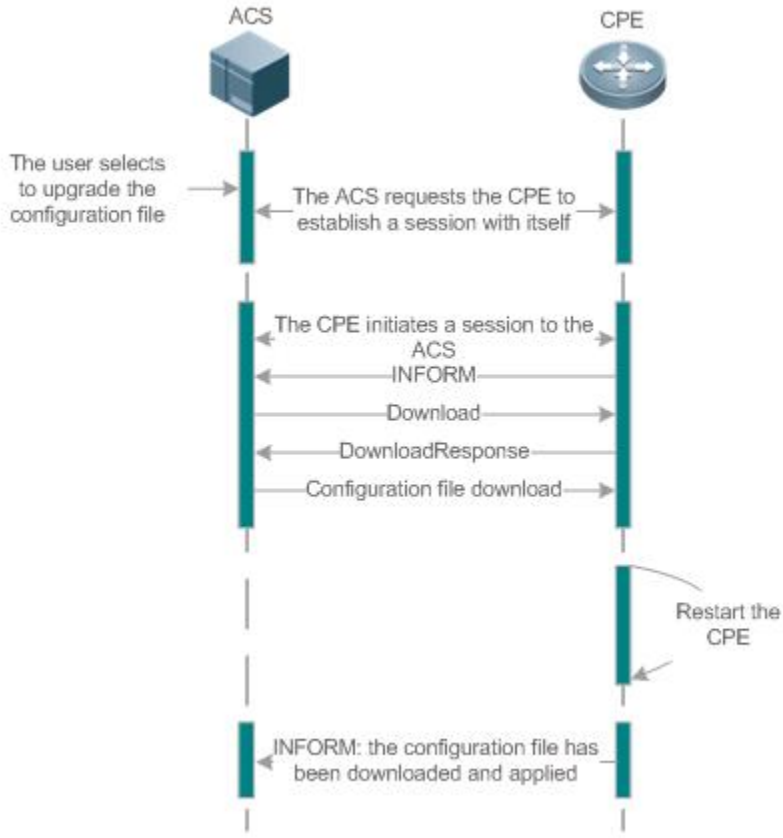
The file server can be ACS or separately deployed.

7.3.2 Upgrading the Configuration Files

Upgrading the Configuration Files means the current configuration files of a CPE can be replaced with specified configuration files, so that the new configuration files act on the CPE after reset.

Working Principle

Figure 7- 4



Users specify a CPE for the ACS to deliver the Download methods for upgrading its configuration files. The CPE downloads the configuration files from the specified file server, upgrade configuration files, and then reboot. After that, the CPE will indicate successful or unsuccessful completion of the method application.

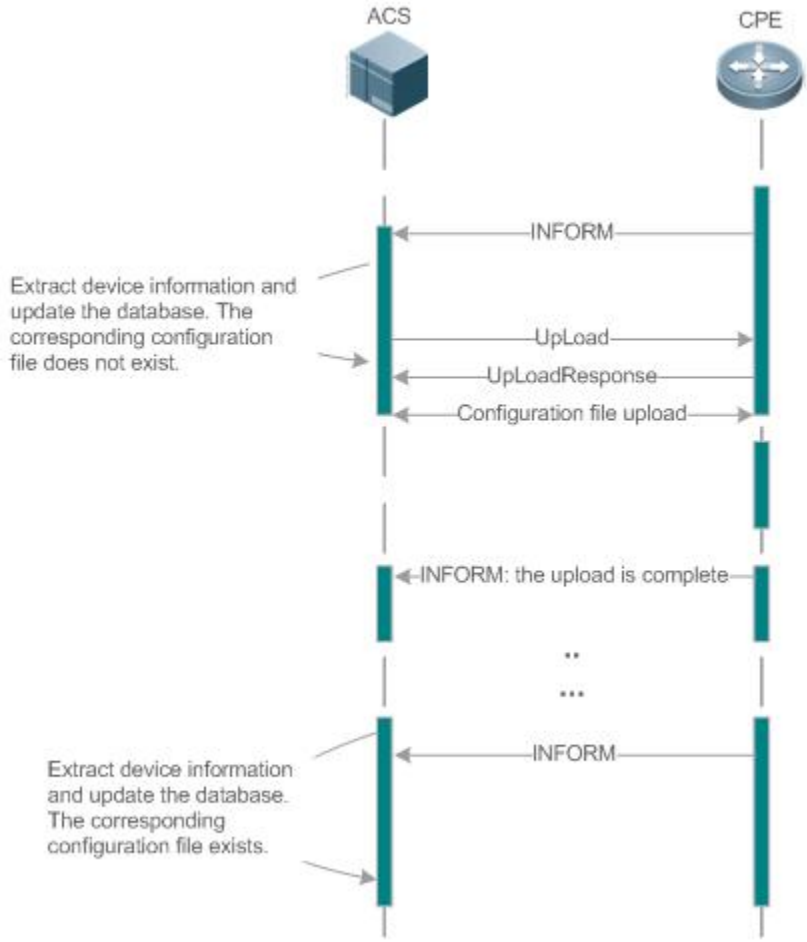
The file server can be ACS or separately deployed.

7.3.3 Uploading the Configuration Files

Uploading the Configuration Files means the ACS controls the configuration files of CPEs by using the Upload method.

Working Principle

Figure 7- 5



When a CPE initially accesses the ACS, the ACS attempts to learn the configuration files of the CPE in the following sequence:

- When the ACS initially receives an Inform message from the CPE, it locates the corresponding database information according to device information carried in the message.
- If the database does not contain the configuration files of the CPE, the ACS delivers the Upload method to the CPE for uploading the configuration files.
- The CPE uploads its current configuration files to the ACS.
- The CPE returns a successful or unsuccessful response to the Upload request.

7.3.4 Backing Up and Restoring a CPE

When a remote CPE breaks away from the management center due to abnormal operations, the CPE backup and restoration feature helps restore the CPE to the previous status, so that the management center can resume the supervision of the CPE as necessary.

Working Principle

You can configure the restoration function on a CPE, so that the CPE can restore itself from exceptions of its firmware or configuration files. Then when the CPE fails to connect to the ACS and breaks away from the management center after its firmware or configuration files are upgraded, the previous firmware or configuration files of the CPE can be restored in time for the ACS to manage the CPE. This kind of exception is generally caused by delivery of a wrong version or configuration file.

Before the CPE receives a new firmware or configuration files to upgrade, the CPE will back up its current version and configuration files. In addition, there is a mechanism for determining whether the problem described in the preceding scenario has occurred. If the problem has occurred, the CPE is restored to the previous manageable status.

7.4 Configuration

Action	Suggestions and Related Commands	
Establishing a Basic CWMP Connection	(Mandatory) You can configure the ACS or CPE usernames and passwords to be authenticated for CWMP connection.	
	cwmp	Enables CWMP and enters CWMP configuration mode.
	acs username	Configures the ACS username for CWMP connection.
	acs password	Configures the ACS password for CWMP connection.
	cpe username	Configures the CPE username for CWMP connection.
	cpe password	Configures the CPE password for CWMP connection.
	(Optional)_You can configure the URLs of the CPE and the ACS.	
	acs url	Configures the ACS URL.
	cpe url	Configures the CPE URL.
Configuring CWMP-Related Attributes	(Optional) You can configure the basic functions of the CPE, such as upload, backup and restoration of firmware, configuration files or logs.	
	cpe inform	Configures the periodic notification function of the CPE.
	cpe back-up	Configures the backup and restoration of the firmware and configuration file of the CPE.
	disable download	Disables the function of downloading firmware and configuration files from the ACS.
	disable upload	Disables the function of uploading configuration and log files to the ACS.
	timer cpe- timeout	Configures the ACS response timeout on CPEs.

7.4.1 Establishing a Basic CWMP Connection

Configuration Effect

- A session connection is established between the ACS and the CPE.

Precautions

- N/A

Configuration Method

Enabling CWMP and Entering CWMP Configuration Mode

- (Mandatory) The CWMP function is enabled by default.

Command	**cwmp**
Parameter Description	N/A
Defaults	CWMP is enabled by default.
Command Mode	Global configuration guide
Usage Guide	N/A

Configuring the ACS Username for CWMP Connection

- This configuration is mandatory on the ACS.
- Only one username can be configured for the ACS. If multiple are configured, the latest configuration is applied.

Command	**acs username** *username*
Parameter Description	**username** *username*: The ACS username for CWMP connection
Defaults	The ACS username is not configured by default.
Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the ACS Password for CWMP Connection

- This configuration is mandatory on the ACS.
- The password of the ACS can be in plaintext or encrypted form. Only one password can be configured for the ACS. If multiple are configured, the latest configuration is applied.

Command	**acs password** {*password* | *encryption-type encrypted-password*}
Parameter Description	*password:* ACS password *encryption-type:* 0 (no encryption) or 7 (simple encryption)

	encrypted-password: Password text
Defaults	*encryption-type*: 0 *encrypted-password*: N/A
Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the CPE Username for CWMP Connection

- This configuration is mandatory on the CPE.
- Only one username can be configured for the CPE. If multiple are configured, the latest configuration is applied.

Command	**cpe username** *username*
Parameter Description	*username*: CPE username
Defaults	No CPE username is configured by default.
Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the CPE Password for CWMP Connection

- This configuration is mandatory on the CPE.
- The password of the CPE can be in plaintext or encrypted form. Only one password can be configured for the CPE. If multiple are configured, the latest configuration is applied.

Command	**cpe password** {*password* | *encryption-type encrypted-password*}
Parameter Description	*password:* CPE password *encryption-type:* 0 (no encryption) or 7 (simple encryption) *encrypted-password:* Password text
Defaults	*encryption-type*: 0 *encrypted-password*: N/A
Command Mode	CWMP configuration mode
Usage Guide	Use this command to configure the CPE user password to be authenticated for the ACS to connect to the CPE. In general, the encryption type does not need to be specified. The encryption type needs to be specified only when copying and pasting the encrypted password of this command. A valid password should meet the following format requirements: ● Contain 1 to 26 characters including letters and figures. ● The leading spaces will be ignored, while the trailing and middle are valid. ● If 7 (simple encryption) is specified, the valid characters only include 0 to 9 and a (A) to f (F).

Configuring the ACS URL for CMWP Connection

- This configuration is optional on the CPE.
- Only one ACS URL can be configured. If multiple are configured, the latest configuration is applied. The ACS URL must be in HTTP format.

Command	**acs url** *url*
Parameter Description	*url*: ACS URL
Defaults	No ACS URL is configured by default.
Command Mode	CWMP configuration mode
Usage Guide	If the ACS URL is not configured but obtained through DHCP, CPEs will use this dynamic URL to initiate connection to the ACS. The ACS URL must: ● Be in format of **http://host[:port]/path** or **https://host[:port]/path**. ● Contain 256 characters at most.

Configuring the CPE URL for CWMP Connection

- This configuration is optional on the CPE.
- Only one CPE URL can be configured. If multiple are configured, the latest configuration is applied. The CPE URL must be in HTTP format instead of domain name format.

Command	**cpe url** *url*
Parameter Description	*url:* CPE URL
Defaults	No CPE URL is configured by default.
Command Mode	CWMP configuration mode
Usage Guide	If CPE URL is not configured, it is obtained through DHCP. The CPE URL must: ● Be in format of **http://ip [: port]/**. ● Contain 256 characters at most.

Configuration Examples

The following configuration examples describe CWMP-related configuration only.

Configuring Usernames and Passwords on the CPE

Network Environment Figure 7- 6	

Configuration Method	● Enable CWMP. ● On the CPE, configure the ACS username and password to be authenticated for the CPE to connect to the ACS. ● On the CPE, configure the CPE username and password to be authenticated for the ACS to connect to the CPE.
CPE	FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# cwmp FS(config-cwmp)# acs username USERB FS(config-cwmp)# acs password PASSWORDB FS(config-cwmp)# cpe username USERB FS(config-cwmp)# cpe password PASSWORDB
Verification	● Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	FS# show cwmp configuration CWMP Status : enable ACS URL : http://10.10.10.1:7547/acs ACS username : USERA ACS password : ****** CPE URL : http://10.10.10.2:7547/ CPE username : USERB CPE password : ******

Configuring the URLs of the ACS and the CPE

Network Environment	See Figure 7- 6.
Configuration Method	● Configure the ACS URL. ● Configure the CPE URL.
CPE	FS# configure terminal FS(config)# cwmp FS(config-cwmp)# acs url http://10.10.10.1:7547/acs FS(config-cwmp)# cpe url http://10.10.10.1:7547/
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	FS#show cwmp configuration CWMP Status : enable

Network Environment	See Figure 7- 6.
Configuration Method	● Configure the ACS URL. ● Configure the CPE URL.
CPE	FS# configure terminal FS(config)# cwmp FS(config-cwmp)# acs url http://10.10.10.1:7547/acs FS(config-cwmp)# cpe url http://10.10.10.1:7547/
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
	ACS URL : http://10.10.10.1:7547/acs ACS username : USERA ACS password : ****** CPE URL : http://10.10.10.2:7547/

Common Errors

- The user-input encrypted password is longer than 254 characters, or the length of the password is not an even number.
- The user-input plaintext password is longer than 100 characters.
- The user-input plaintext password contains illegal characters.
- The user-input encrypted password contains illegal characters (the legitimate characters includes only 0~9, a~f and A~F)
- The URL of the ACS is set to NULL.
- The URL of the CPE is set to NULL.

7.4.2 Configuring CWMP-Related Attributes

Configuration Effect

- You can configure common functions of the CPE, such as the backup and restoration of its firmware or configuration file, whether to enable the CPE to download firmware and configuration files from the ACS, and whether to enable the CPE to upload its configuration and log files to the ACS.

Configuration Method

Configuring the Periodic Notification Function of the CPE

- (Optional) The value range is from 30 to 3,600 in seconds. The default value is 600 seconds.
- Perform this configuration to reset the periodical notification interval of the CPE.

Command	**cpe inform** [**interval** *seconds*] [**starttime** *time*]
Parameter	*seconds*: Specifies the periodical notification interval of the CPE. The value range is from 30 to 3,600 in seconds.

Description	*time*: Specifies the date and time for starting periodical notification in *yyyy-mm-ddThh:mm:ss* format.
Command Mode	CWMP configuration mode
Defaults	The default value is 600 seconds.
Usage Guide	Use this command to configure the periodic notification function of the CPE. ● If the time for starting periodical notification is not specified, periodical notification starts after the periodical notification function is enabled. The notification is performed once within every notification interval. ● If the time for starting periodical notification is specified, periodical notification starts at the specified start time. For instance, if the periodical notification interval is set to 60 seconds and the start time is 12:00 am next day, periodical notification will start at 12:00 am next day and once every 60 seconds.

Disabling the Function of Downloading Firmware and Configuration Files from the ACS

- (Optional) The CPE can download firmware and configuration files from the ACS by default.
- Perform this configuration if the CPE does not need to download firmware and configuration files from the ACS.

Command	**disable download**
Parameter Description	N/A
Defaults	The CPE can download firmware and configuration files from the ACS by default.
Command Mode	CWMP configuration mode
Usage Guide	Use this command to disable the function of downloading main program and configuration files from the ACS. ● This command does not act on configuration script files. The configuration scripts can still be executed even if this function is disabled.

Disabling the Function of Uploading Configuration and Log Files to the ACS

- (Optional.) The CPE can upload configuration and log files to the ACS by default.
- Perform this configuration if the CPE does not need to upload configuration and log files to the ACS.

Command	**disable upload**
Parameter Description	N/A
Defaults	The CPE can upload configuration and log files to the ACS by default.
Command Mode	CWMP configuration mode
Usage Guide	Use this command to disable the function of uploading configuration and log files to the ACS.

Configuring the Backup and Restoration of the Firmware and Configuration Files of the CPE

- (Optional) The backup and restoration of the firmware and configuration files of the CPE is enabled by default. The value range is from 30 to 10,000 in seconds. The default value is 60 seconds.
- The longer the delay-time is, the longer the reboot will be complete.
- Perform this configuration to modify the function of backing up and restoring the firmware and configuration files of the CPE.

Command	**cpe back-up** [**delay-time** *seconds*]
Parameter Description	*seconds*: Specifies the delay for backup and restoration of the firmware and configuration file of the CPE.
Defaults	The default value is 60 seconds.
Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the ACS Response Timeout

- (Optional) The value range is from 10 to 600 in seconds. The default value is 30 seconds.
- Perform this configuration to modify the ACS response timeout period on the CPE.

Command	**timer cpe- timeout** *seconds*
Parameter Description	*seconds*: Specifies the timeout period in seconds. The value range is from 10 to 600.
Defaults	The default value is 30 seconds.
Command Mode	CWMP configuration mode
Usage Guide	N/A

Verification

- Run the show cwmp configuration command.

Command	**show cwmp configuration**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A
Configuration Examples	The following example displays the CWMP configuration. FS(config-cwmp)#show cwmp configuration CWMP Status : enable ACS URL : http://www.FS.com.cn/acs ACS username : admin

	ACS password : ****** CPE URL : http://10.10.10.2:7547/ CPE username : FS CPE password : ****** CPE inform status : disable CPE inform interval : 60s CPE inform start time : 0:0:0 0 0 0 CPE wait timeout : 50s CPE download status : enable CPE upload status : enable CPE back up status : enable CPE back up delay time : 60s

Configuration Examples

Configuring the Periodical Notification Interval of the CPE

Network Environment	See Figure 7-6.
Configuration Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Set the periodical notification interval of the CPE to 60 seconds.
CPE	FS#config Enter configuration commands, one per line. End with CNTL/Z. FS(config)#cwmp FS(config-cwmp)#cpe inform interval 60
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	FS#show cwmp configuration CWMP Status : enable …… CPE inform interval : 60s

Disabling the Function of Downloading Firmware and Configuration Files from the ACS

Network Environment	See Figure 7-6.

Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Disable the function of downloading firmware and configuration files from the ACS.
CPE	FS#config Enter configuration commands, one per line. End with CNTL/Z. FS(config)#cwmp FS(config-cwmp)#disable download
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	FS#show cwmp configuration CWMP Status : enable …… CPE download status : disable

Disabling the Function of Uploading Configuration and Log Files to the ACS

Network Environment	See Figure 7- 6.
Configuration Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Disable the CPE's function of uploading configuration and log files to the ACS.
CPE	FS#config Enter configuration commands, one per line. End with CNTL/Z. FS(config)#cwmp FS(config-cwmp)# disable upload
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	FS#show cwmp configuration CWMP Status : enable …… CPE upload status : disable

Configuring the Backup and Restoration Delay

Network Environment	See Figure 7- 6.

Configuration Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Set the backup and restoration delay to 100 seconds.
CPE	FS#config Enter configuration commands, one per line. End with CNTL/Z. FS(config)#cwmp FS(config-cwmp)# cpe back-up Seconds 30
Verification	● Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	FS#show cwmp configuration CWMP Status : enable …… CPE back up delay time : 30s

Configuring the ACS Response Timeout of the CPE

Network Environment	See Figure 7- 6.
Configuration Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Set the response timeout of the CPE to 100 seconds.
CPE	FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# cwmp FS(config-cwmp)# timer cpe-timeout 100
Verification	● Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	FS#show cwmp configuration CWMP Status : enable …… CPE wait timeout : 100s

Common Errors

N/A

7.5 Monitoring

Displaying

Command	Function
show cwmp configuration	Displays the CWMP configuration.
show cwmp status	Displays the CWMP running status.

8 Configuring Syslog

8.1 Overview

Status changes (such as link up and down) or abnormal events may occur anytime. FSproducts provide the syslog mechanism to automatically generate messages (log packets) in fixed format upon status changes or occurrence of events. These messages are displayed on the related windows such as the Console or monitoring terminal, recorded on media such as the memory buffer or log files, or sent to a group of log servers on the network so that the administrator can analyze network performance and identify faults based on these log packets. Log packets can be added with the timestamps and sequence numbers and classified by severity level so that the administrator can conveniently read and manage log packets.

Protocols and Standards

- RFC3164: The BSD syslog Protocol
- RFC5424: The_Syslog_Protocol

8.2 Applications

Application	Description
Sending Syslogs to the Console	Monitor syslogs through the Console.
Sending Syslogs to the Log Server	Monitor syslogs through the server.

8.2.1 Sending Syslogs to the Console

Scenario

Send syslogs to the Console to facilitate the administrator to monitor the performance of the system. The requirements are as follows:

1. Send logs of Level 6 or higher to the Console.
2. Send logs of only the ARP and IP modules to the Console.

Figure 8- 1 shows the network topology.

Figure 8- 1 Network topology

Deployment

Configure the device as follows:

1. Set the level of logs that can be sent to the Console to informational (Level 6).
2. Set the filtering direction of logs to terminal.
3. Set log filtering mode of logs to contains-only.
4. Set the filtering rule of logs to single-match. The module name contains only ARP or IP.

8.2.2 Sending Syslogs to the Log Server

Scenario

Send syslogs to the log server to facilitate the administrator to monitor the logs of devices on the server. The requirements are as follows:

1. Send syslogs to the log server 10.1.1.1.
2. Send logs of Level 7 or higher to the log server.
3. Send syslogs from the source interface Loopback 0 to the log server.

Figure 8- 2 shows the network topology.

Figure 8- 2 Network topology

Deployment

Configure the device as follows:

1. Set the IPv4 address of the server to 10.1.1.1.
2. Set the level of logs that can be sent to the log server to debugging (Level 7).
3. Set the source interface of logs sent to the log server to Loopback 0.

8.3 Features

Basic Concepts

Classification of Syslogs

Syslogs can be classified into two types:

- Log type
- Debug type

Levels of Syslogs

Eight severity levels of syslogs are defined in descending order, including emergency, alert, critical, error, warning, notification, informational, and debugging. These levels correspond to eight numerical values from 0 to 7. A smaller value indicates a higher level.

Only logs with a level equaling to or higher than the specified level can be output. For example, if the level of logs is set to informational (Level 6), logs of Level 6 or higher will be output.

The following table describes the log levels.

Level	Numerical Value	Description
emergencies	0	Indicates that the system cannot run normally.
alerts	1	Indicates that the measures must be taken immediately.

critical	2	Indicates a critical condition.
errors	3	Indicates an error.
warnings	4	Indicates a warning.
notifications	5	Indicates a notification message that requires attention.
informational	6	Indicates an informational message.
debugging	7	Indicates a debugging message.

Output Direction of Syslogs

Output directions of syslogs include Console, monitor, server, buffer, and file. The default level and type of logs vary with the output direction. You can customize filtering rules for different output directions.

The following table describes output directions of syslogs.

Output Direction	Description	Default Output Level	Description
Console	Console	Debugging (Level 7)	Logs and debugging information are output.
monitor	Monitoring terminal	Debugging (Level 7)	Logs and debugging information are output.
server	Log server	Informational (Level 6)	Logs and debugging information are output.
buffer	Log buffer	Debugging (Level 7)	Logs and debugging information are output. The log buffer is used to store syslogs.
file	Log file	Informational (Level 6)	Logs and debugging information are output. Logs in the log buffer are periodically written into files.

RFC3164 Log Format

Formats of syslogs may vary with the syslog output direction.

- If the output direction is the Console, monitor, buffer, or file, the syslog format is as follows:

```
seq no: *timestamp: sysname %module-level-mnemonic: content
```

For example, if you exit configuration mode, the following log is displayed on the Console:

```
001233: *May 22 09:44:36: FS%SYS-5-CONFIG_I: Configured from console by console
```

- If the output direction is the log server, the syslog format is as follows:

```
<priority>seq no: *timestamp: sysname %module-level-mnemonic: content
```

For example, if you exit configuration mode, the following log is displayed on the log server:

```
<189>001233: *May 22 09:44:36: FS%SYS-5-CONFIG_I: Configured from console by console
```

The following describes each field in the log in details:

4. Priority

This field is valid only when logs are sent to the log server.

The priority is calculated using the following formula: Facility x 8 + Level Level indicates the numerical code of the log level and Facility indicates the numerical code of the facility. The default facility value is local7 (23). The following table lists the value range of the facility.

Numerical Code	Facility Keyword	Facility Description
0	kern	kernel messages
1	user	user-level messages
2	mail	mail system
3	daemon	system daemons
4	auth1	security/authorization messages
5	syslog	messages generated internally by syslogs
6	lpr	line printer subsystem
7	news	network news subsystem
8	uucp	UUCP subsystem
9	clock1	clock daemon
10	auth2	security/authorization messages
11	ftp	FTP daemon
12	ntp	NTP subsystem
13	logaudit	log audit
14	logalert	log alert
15	clock2	clock daemon
16	local0	local use 0 (local0)
17	local1	local use 1 (local1)
18	local2	local use 2 (local2)
19	local3	local use 3 (local3)
20	local4	local use 4 (local4)
21	local5	local use 5 (local5)
22	local6	local use 6 (local6)
23	local7	local use 7 (local7)

5. Sequence Number

The sequence number of a syslog is a 6-digit integer, and increases sequentially. By default, the sequence number is not displayed. You can run a command to display or hide this field.

6. Timestamp

The timestamp records the time when a syslog is generated so that you can display and check the system event conveniently. FSdevices support two syslog timestamp formats: datetime and uptime.

If the device does not have the real time clock (RTC), which is used to record the system absolute time, the device uses its startup time (uptime) as the syslog timestamp by default. If the device has the RTC, the device uses its absolute time (datetime) as the syslog timestamp by default.

The two timestamp formats are described as follows:

- Datetime format

The datetime format is as follows:

```
Mmm dd yyyy hh:mm:ss.msec
```

The following table describes each parameter of the datetime.

Timestamp Parameter	Parameter Name	Description
Mmm	Month	Mmm refers to abbreviation of the current month. The 12 months in a year are written as Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec.
dd	Day	dd indicates the current date.
yyyy	Year	yyyy indicates the current year, and is not displayed by default.
hh	Hour	hh indicates the current hour.
mm	Minute	mm indicates the current minute.
ss	Second	ss indicates the current second.
msec	Millisecond	msec indicates the current millisecond.

By default, the datetime timestamp displayed in the syslog does not contain the year and millisecond. You can run a command to display or hide the year and millisecond of the datetime timestamp.

- Uptime format

The uptime format is as follows:

```
dd:hh:mm:ss
```

The timestamp string indicates the accumulated days, hours, minutes, and seconds since the system is started.

7. Sysname

This field indicates the name of the device that generates the log so that the log server can identify the host that sends the log. By default, this field is not displayed. You can run a command to display or hide this field.

8. Module

This field indicates the name of the module that generates the log. The module name is an upper-case string of 2 to 20 characters, which contain upper-case letters, digits, or underscores. The module field is mandatory in the log-type information, and optional in the debug-type information.

9. Level

Eight syslog levels from 0 to 7 are defined. The level of syslogs generated by each module is fixed and cannot be modified.

10. Mnemonic

This field indicates the brief information about the log. The mnemonic is an upper-case string of 4 to 32 characters, which may include upper-case letters, digits, or underscore. The mnemonic field is mandatory in the log-type information, and optional in the debug-type information.

11. Content

This field indicates the detailed content of the syslog.

RFC5424 Log Format

The syslog format in the output direction is as follows:

```
<priority>version timestamp sysname MODULE LEVEL MNEMONIC [structured-data] description
```

For example, if you exit configuration mode, the following log is displayed on the Console:

```
<133>1 2013-07-24T12:19:33.130290Z FSSYS 5 CONFIG - Configured from console by console
```

The following describes each field in the log in details:

12. Priority

The priority is calculated using the following formula: Facility x 8 + Level. Level indicates the numerical code of the log level and Facility indicates the numerical code of the facility. When the RFC5424 format is enabled, the default value of the facility field is local0 (16).

13. Version

According to RFC5424, the version is always 1.

14. Timestamp

The timestamp records the time when a syslog is generated so that you can display and check the system event conveniently. FSdevices use the following uniformed timestamp format when the RFC5424 logging function is enabled:

```
YYYY-MM-DDTHH:MM:SS.SECFRACZ
```

The following table describes each parameter of the timestamp.

Timestamp Parameter	Description	Remark
YYYY	Year	YYYY indicates the current year.
MM	Month	MM indicates the current month.
DD	Day	DD indicates the current date.
T	Separator	The date must end with "T".
HH	Hour	HH indicates the current hour.
MM	Minute	MM indicates the current minute.
SS	Second	SS indicates the current second.
SECFRAC	Millisecond	SECFRAC indicates the current millisecond (1–6 digits).
Z	End mark	The time must end with "Z".

15. Sysname

This field indicates the name of the device that generates the log so that the log server can identify the host that sends the log.

16. Module

This field indicates the name of the module that generates the log. The module name is an upper-case string of 2 to 20 characters, which contain upper-case letters, digits, or underscores. The module field is mandatory in the log-type information, and optional in the debug-type information.

17. Level

Eight syslog levels from 0 to 7 are defined. The level of syslogs generated by each module is fixed and cannot be modified.

18. Mnemonic

This field indicates the brief information about the log. The mnemonic is an upper-case string of 4 to 32 characters, which contain upper-case letters, digits, or underscores. The Mnemonic field is mandatory in the log-type information, and optional in the debug-type information.

19. Structured-Data

Structured-data introduced in RFC5424 is parsed as a whole string containing parameter information. Each log may contain 0 or multiple parameters. If a parameter is null, replace this parameter with a placeholder (-). The format of this field is as follows:

```
[SD_ID@enterpriseID PARAM-NAME=PARAM-VALUE]
```

The following table describes each parameter of the structured-data field.

Parameter in structured-data	Description	Remarks
SD_ID	Parameter information name	The parameter information name is capitalized, and must be unique in a log.
@	Separator	"@enterpriseID" is added only to the customized parameter information, not to the parameter information defined in RFC5424.
enterpriseID	Enterprise ID	The enterprise ID is maintained by the Internet Assigned Numbers Authority (IANA). FSNetworks' enterprise ID is 4881. You can query the enterprise ID on the official website of IANA. http://www.iana.org/assignments/enterprise-numbers
PARAM-NAME	Parameter name	The parameter name is capitalized, and must be unique in the structured-data of a log.
PARAM-VALUE	Parameter value	The parameter value must be enclosed in double quotation marks. Values of the IP address or MAC address must be capitalized, and other types of values are capitalized as required.

20. description

This field indicates the content of the syslog.

Overview

Feature	Description
Logging	Enable or disable the system logging functions.
Syslog Format	Configure the syslog format.
Logging Direction	Configure the parameters to send syslogs in different directions.
Syslog Filtering	Configure parameters of the syslog filtering function.
Featured Logging	Configure parameters of the featured logging function.
Syslog Monitoring	Configure parameters of the syslog monitoring function.

8.3.1 Logging

Enable or disable the logging, log redirection, and log statistics functions.

Related Configuration

Enable Logging

By default, logging is enabled.

Run the **logging on** command to enable logging in global configuration mode. After logging is enabled, logs generated by the system are sent in various directions for the administrator to monitor the performance of the system.

Enabling Log Statistics

By default, log statistics is disabled.

Run the **logging count** command to enable log statistics in global configuration mode. After log statistics is enabled, the system records the number of times a log is generated and the last time when the log is generated.

8.3.2 Syslog Format

Configure the syslog format, including the RFC5424 log format, timestamp format, sysname, and sequence number.

Related Configuration

Enabling the RFC5424 Log Format

By default, the RFC5424 log format is disabled.

After the new format (RFC5424 log format) is enabled, the service sequence-numbers, service sysname, service **timestamps**, **service private-syslog**, and **service standard-syslog** that are applicable only to the old format (RFC3164 log format) lose effect and are hidden.

After the old format (RFC3164 log format) is enabled, the logging delay-send, logging policy, and logging statistic commands that are applicable only to the RFC5424 log format lose effect and are hidden.

After log format switchover, the outputs of the show logging and show logging config commands change accordingly.

Configuring the Timestamp Format

By default, the syslog uses the datetime timestamp format, and the timestamp does not contain the year and millisecond.

Run the **service timestamps** command in global configuration mode to use the datetime timestamp format that contains the year and millisecond in the syslog, or change the datetime format to the uptime format.

Adding Sysname to the Syslog

By default, the syslog does not contain sysname.

Run the **service sysname** command in global configuration mode to add sysname to the syslog.

Adding the Sequence Number to the Syslog

By default, the syslog does not contain the sequence number.

Run the **service sequence-numbers** command in global configuration mode to add the sequence number to the syslog.

Enabling the Standard Log Format

By default, logs are displayed in the following format:

```
*timestamp: %module-level-mnemonic: content
```

Run the **service standard-syslog** command in global configuration mode to enable the standard log format and logs are displayed in the following format:

```
timestamp %module-level-mnemonic: content
```

Compared with the default log format, an asterisk (*) is missing in front of the timestamp, and a colon (:) is missing at the end of the timestamp in the standard log format.

Enabling the Private Log Format

By default, logs are displayed in the following format:

```
*timestamp: %module-level-mnemonic: content
```

Run the **service private-syslog** command in global configuration mode to enable the private log format and logs are displayed in the following format:

```
timestamp module-level-mnemonic: content
```

Compared with the default log format, an asterisk (*) is missing in front of the timestamp, a colon (:) is missing at the end of the timestamp, and a percent sign (%) is missing at the end of the module name in the private log format.

8.3.3 Logging Direction

Configure parameters for sending syslogs in different directions, including the Console, monitor terminal, buffer, the log server, and log files.

Related Configuration

Synchronizing User Input with Log Output

By default, this function is disabled.

Run the **logging synchronous** command in line configuration mode to synchronize user input with log output. After this function is enabled, user input will not be interrupted.

Configuring the Log Rate Limit

By default, no log rate limit is configured.

Run the **logging rate-limit** { *number* | **all** *number* | **console** {*number* | **all** *number*} } [**except** [*severity*]] command in global configuration mode to configure the log rate limit.

Configuring the Level of Logs Sent to the Console

By default, the level of logs sent to the Console is debugging (Level 7).

Run the **logging console** [*level*] command in global configuration mode to configure the level of logs that can be sent to the Console.

Sending Logs to the Monitor Terminal

By default, it is not allowed to send logs to the monitor terminal.

Run the **terminal monitor** command in the privileged EXEC mode to send logs to the monitor terminal.

Configuring the Level of Logs Sent to the Monitor Terminal

By default, the level of logs sent to the monitor terminal is debugging (Level 7).

Run the **logging monitor** [*level*] command in global configuration mode to configure the level of logs that can be sent to the monitor terminal.

Writing Logs into the Memory Buffer

By default, logs are written into the memory buffer, and the default level of logs is debugging (Level 7).

Run the **logging buffered** [*buffer-size*] [*level*] command in global configuration mode to configure parameters for writing logs into the memory buffer, including the buffer size and log level.

Sending Logs to the Log Server

By default, logs are not sent to the log server.

Run the **logging server** [**oob**] { *ip-address* } [**udp-port** *port*] command in global configuration mode to send logs to a specified log server.

Configuring the Level of Logs Sent to the Log Server

By default, the level of logs sent to the log server is informational (Level 6).

Run the **logging trap** [*level*] command in global configuration mode to configure the level of logs that can be sent to the log server.

Configuring the Facility Value of Logs Sent to the Log Server

If the RFC5424 log format is disabled, the facility value of logs sent to the log server is local7 (23) by default. If the RFC5424 log format is enabled, the facility value of logs sent to the log server is local0 (16) by default.

Run the **logging facility** *facility-type* command in global configuration mode to configure the facility value of logs sent to the log server.

Configuring the Source Address of Logs Sent to the Log Server

By default, the source address of logs sent to the log server is the IP address of the interface sending logs.

Run the **logging source** [**interface**] *interface-type interface-number* command to configure the source interface of logs. If this source interface is not configured, or the IP address is not configured for this source interface, the source address of logs is the IP address of the interface sending logs.

Run the **logging source** { **ip** *ip-address* } command to configure the source IP address of logs. If this IP address is not configured on the device, the source address of logs is the IP address of the interface sending logs.

Writing Logs into Log Files

By default, logs are not written into log files. After the function of writing logs into log files is enabled, the level of logs written into log files is informational (Level 6) by default.

Run the **logging file** { **sata0:***filename* | **flash:***filename* | **usb0**:*filename* | **usb1**:*filename* } [*max-file-size*] [level] command in global configuration mode to configure parameters for writing logs into log files, including the type of device where the file is stored, file name, file size, and log level.

Configuring the Number of Log Files

By default, the number of log files is 16.

Run the **logging file numbers** *numbers* command in global configuration mode to configure the number of log files.

Configuring the Interval at Which Logs Are Written into Log Files

By default, logs are written into log files at the interval of 3600s (one hour).

Run the **logging flash interval** *seconds* command in global configuration mode to configure the interval at which logs are written into log files.

Configuring the Storage Time of Log Files

By default, the storage time is not configured.

Run the **logging life-time level** *level days* command in global configuration mode to configure the storage time of logs. The administrator can specify different storage days for logs of different levels.

Immediately Writing Logs in the Buffer into Log Files

By default, syslogs are stored in the syslog buffer and then written into log files periodically or when the buffer is full.

Run the **logging flash flush** command in global configuration mode to immediately write logs in the buffer into log files so that you can collect logs conveniently.

8.3.4 Syslog Filtering

By default, logs generated by the system are sent in all directions.

Working Principle

Filtering Direction

Five log filtering directions are defined:

- buffer: Filters out logs sent to the log buffer, that is, logs displayed by the show logging command.
- file: Filters out logs written into log files.
- server: Filters out logs sent to the log server.
- terminal: Filters out logs sent to the Console and monitor terminal (including Telnet and SSH).

The four filtering directions can be used either in combinations to filter out logs sent in various directions, or separately to filter out logs sent in a single direction.

Filtering Mode

Two filtering modes are available:

- contains-only: Indicates that only logs that contain keywords specified in the filtering rules are output. You may be interested in only a specified type of logs. In this case, you can apply the contains-only mode on the device to display only logs that match filtering rules on the terminal, helping you check whether any event occurs.
- filter-only: Indicates that logs that contain keywords specified in the filtering rules are filtered out and will not be output. If a module generates too many logs, spamming may occur on the terminal interface. If you do not care about this type of logs, you can apply the filter-only mode and configure related filtering rules to filter out logs that may cause spamming.

The two filtering modes are mutually exclusive, that is, you can configure only one filtering mode at a time.

Filter Rule

Two filtering rules are available:

- exact-match: If exact-match is selected, you must select all the three filtering options (module, level, and mnemonic). If you want to filter out a specified log, use the exact-match filtering rule.
- single-match: If exact-match is selected, you only need to select one of the three filtering options (module, level, and mnemonic). If you want to filter out a specified type of logs, use the single-match filtering rule.

If the same module, level, or mnemonic is configured in both the single-match and exact-match rules, the single-match rule prevails over the exact-match rule.

Related Configuration

Configuring the Log Filtering Direction

By default, the log filtering direction is all, that is, logs sent in all directions are filtered.

Run the **logging filter direction** { **all** | **buffer** | **file** | **server** | **terminal** } command in global configuration mode to configure the log filtering direction to filter out logs in the specified directions.

Configuring the Log Filtering Mode

By default, the log filtering mode is filter-only.

Run the **logging filter type** { **contains-only** | **filter-only** } command in global configuration mode to configure the log filtering mode.

Configuring the Log Filtering Rule

By default, no log filtering rule is configured on a device, that is, logs are not filtered out.

Run the **logging filter rule exact-match module** *module-name* **mnemonic** *mnemonic-name* **level** *level* command in global configuration mode to configure the exact-match rule.

Run the **logging filter rule single-match** { **level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name* } command in global configuration mode to configure the single-match rule.

8.3.5 Featured Logging

The featured logging functions include level-based logging, delayed logging, and periodical logging. If the RFC5424 log format is enabled, logs can be sent in all directions, delayed logging is enabled, and periodical logging is disabled by default. If the RFC5424 log format is disabled, level-based logging, delayed logging, and periodical logging are disabled.

Working Principle

Level-based Logging

You can use the level-based logging function to send syslogs to different destinations based on different module and severity level. For example, you can configure commands to send WLAN module logs of Level 4 or lower to the log server, and WLAN module logs of Level 5 or higher to local log files.

Delayed Logging

After generated, logs are not directly sent to the log server, and instead they are buffered in the log file. The device sends the log file to the syslog server through FTP at a certain interval. This function is called delayed logging.

If the device generates too many logs, sending all logs to the server in real time may deteriorate the performance of the device and the syslog server, and increase the burden of the network. In this case, the delayed logging function can be used to reduce the packet interaction.

By default, the log file sent to the remote server is named ***File size_Device IP address_Index*.txt**. If the prefix of the log file name is modified, the log file sent to the remote server is named ***Configured file name prefix_File size_Device IP address_Index*.txt**. The file stored on the local Flash of the device is named ***Configured file name prefix_Index*.txt**. By default, the file name prefix is syslog_ftp_server, the delayed logging interval is 3600s (one hour), and the log file size is 128 KB.

The maximum value of the delayed logging interval is 65535s, that is, 18 hours. If you set the delayed logging interval to the maximum value, the amount of logs generated in this period may exceed the file size (128 KB). To prevent loss of logs, logs will be written into a new log file, and the index increases by 1. When the timer expires, all log files buffered in this period will be sent to the FTP or TFTP server at a time.

The Flash on the device that is used to buffer the local log files is limited in size. A maximum of eight log files can be buffered on the device. If the number of local log files exceeds eight before the timer expires, all log files that are generated earlier will be sent to the FTP or TFTP server at a time.

Periodical Logging

Logs about performance statistics are periodically sent. All periodical logging timers are managed by the syslog module. When the timer expires, the syslog module calls the log processing function registered with each module to output the performance statistic logs and send logs in real time to the remote syslog server. The server analyzes these logs to evaluate the device performance.

By default, the periodical logging interval is 15 minutes. To enable the server to collect all performance statistic logs at a time, you need to set the log periodical logging intervals of different statistic objects to a common multiple of them. Currently, the interval can be set to 0, 15, 30, 60, or 120. 0 indicates that periodical logging is disabled.

Related Configuration

Configuring the Level-based Logging Policy

By default, device logs are sent in all directions.

Run the **logging policy module** *module-name* [**not-lesser-than**] *level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** } command in global configuration mode to configure the level-based logging policy.

Enabling Delayed Display of Logs on the Console and Remote Terminal

By default, delayed display of logs on the Console and remote terminal is disabled.

Run the **logging delay-send terminal** command in global configuration mode to enable delayed display of logs on the Console and remote terminal.

Configuring the Name of the File for Delayed Logging

By default, the log file sent to the remote server is named ***File size_Device IP address_Index*.txt**. If the prefix of the log file name is modified, the log file sent to the remote server is named ***Configured file name prefix_File size_Device IP address_Index*.txt**. The file stored on the local Flash of the device is named ***Configured file name prefix_Index*.txt**. The default file name prefix is syslog_ftp_server.

Run the **logging delay-send file flash:***filename* command in global configuration mode to configure the name of the log file that is buffered on the local device.

Configuring the Delayed Logging Interval

By default, the delayed logging interval is 3600s (one hour).

Run the **logging delay-send interval** *seconds* command in global configuration mode to configure the delayed logging interval.

Configuring the Server Address and Delayed Logging Mode

By default, logs are not sent to any FTP or TFTP server.

Run the **logging delay-send server** { [**oob**] *ip-address* } **mode** { **ftp user** *username* **password** [**0** | **7**] *password* | **tftp** } command in global configuration mode to configure the server address and delayed logging mode.

Enabling Periodical Logging

By default, periodical logging is disabled.

Run the **logging statistic enable** command in global configuration mode to enable periodical uploading of logs. After this function is enabled, the system outputs a series of performance statistics at a certain interval so that the log server can monitor the system performance.

Enabling Periodical Display of Logs on the Console and Remote Terminal

By default, periodical display of logs on the Console and remote terminal is disabled.

Run the **logging statistic terminal** command in global configuration mode to enable periodical display of logs on the Console and remote terminal.

Configuring the Periodical Logging Interval

By default, the periodical logging interval is 15 minutes.

Run the **logging statistic mnemonic** *mnemonic* **interval** *minutes* command in global configuration mode to configure the periodical logging interval.

8.3.6 Syslog Monitoring

After syslog monitoring is enabled, the system monitors the access attempts of users and generates the related logs.

Working Principle

After logging of login/exit attempts is enabled, the system records the access attempts of users. The log contains user name and source address.

After logging of operations is enabled, the system records changes in device configurations, The log contains user name, source address, and operation.

Related Configuration

Enabling Logging of Login or Exit Attempts

By default, a device does not generate logs when users access or exit the device.

Run the **logging userinfo** command in global configuration mode to enable logging of login/exit attempts. After this function is enabled, the device displays logs when users access the devices through Telnet, SSH, or HTTP so that the administrator can monitor the device connections.

Enabling Logging of Operations

By default, a device does not generate logs when users modify device configurations.

Run the **logging userinfo command-log** command in global configuration mode to enable logging of operations. After this function is enabled, the system displays related logs to notify the administrator of configuration changes.

8.4 Configuration

Configuration	Description and Command	
Configuring Syslog Format	(Optional) It is used to configure the syslog format.	
	service timestamps [*message-type* [**uptime**| **datetime** [**msec**] [**year**]]]	Configures the timestamp format of syslogs.
	service sysname	Adds the sysname to the syslog.
	service sequence-numbers	Adds the sequence number to the syslog.
	service standard-syslog	Enables the standard syslog format.
	service private-syslog	Enables the private syslog format.
	service log-format rfc5424	Enables the RFC5424 syslog format.
Sending Syslogs to the Console	(Optional) It is used to configure parameters for sending syslogs to the Console.	
	logging on	Enables logging.
	logging count	Enables log statistics.
	logging console [*level*]	Configures the level of logs displayed on the Console.
	logging rate-limit { *number* | **all** *number* | **console** {*number* | **all** *number* } } [**except** [*severity*]]	Configures the log rate limit.
Sending Syslogs to the Monitor Terminal	(Optional) It is used to configure parameters for sending syslogs to the monitor terminal.	
	terminal monitor	Enables the monitor terminal to display logs.
	logging monitor [*level*]	Configures the level of logs displayed on the monitor terminal.
Writing Syslogs into the Memory Buffer	(Optional) It is used to configure parameters for writing syslogs into the memory buffer.	
	logging buffered [*buffer-size*] [*level*]	Configures parameters for writing syslogs into the memory buffer, including the buffer size and log level.
Sending Syslogs to the Log	(Optional) It is used to configure parameters for sending syslogs to the log server.	

Configuration	Description and Command	
Server	**logging server** [**oob**] { *ip-address* }[**udp-port** *port*]	Sends logs to a specified log server.
	logging trap [*level*]	Configures the level of logs sent to the log server.
	logging facility *facility-type*	Configures the facility value of logs sent to the log server.
	logging source [**interface**] *interface-type interface-number*	Configures the source interface of logs sent to the log server.
	logging source { **ip** *ip-address* }	Configures the source address of logs sent to the log server.
Writing Syslogs into Log Files	(Optional) It is used to configure parameters for writing syslogs into a file.	
	logging file { **sata0:***filename* | **flash:***filename* | **usb0:***filename* | **usb1:***filename* | } [*max-file-size*] [level]	Configures parameters for writing syslogs into a file, including the file storage type, file name, file size, and log level.
	logging file numbers *numbers*	Configures the number of files which logs are written into. The default value is 16.
	logging flash interval *seconds*	Configures the interval at which logs are written into log files. The default value is 3600.
	logging life-time level *level days*	Configures the storage time of log files.
Configuring Syslog Filtering	(Optional) It is used to enable the syslog filtering function.	
	logging filter direction { **all** | **buffer** | **file** | **server** | **terminal** }	Configures the log filtering direction.
	logging filter type { **contains-only** | **filter-only** }	Configures the log filtering mode.
	logging filter rule exact-match module *module-name* **mnemonic** *mnemonic-name* **level** *level*	Configures the exact-match filtering rule.
	logging filter rule single-match { **level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name* }	Configures the single-match filtering rule.
Configuring Level-based Logging	(Optional) It is used to configure logging policies to send the syslogs based on module and severity level .	
	logging policy module *module-name* [**not-lesser-than**] *level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** }	Sends logs to different destinations by module and severity level
Configuring Delayed Logging	(Optional) It is used to enable the delayed logging function.	

Configuration	Description and Command	
	logging delay-send terminal	Enables delayed display of logs on the Console and remote terminal.
	logging delay-send file flash:*filename*	Configures the name of the file on the local device where logs are buffered.
	logging delay-send interval *seconds*	Configures the interval at which logs are sent to the log server.
	logging delay-send server { [**oob**] *ip-address* } **mode** { **ftp user** *username* **password** [**0** | **7**] *password* | **tftp** }	Configures the server address and delayed logging mode.
Configuring Periodical Logging	(Optional) It is used to enable the periodical logging function.	
	logging statistic enable	Enables the periodical logging function .
	logging statistic terminal	Enables periodical display of logs on the Console and remote terminal.
	logging statistic mnemonic *mnemonic* **interval** *minutes*	Configures the interval at which logs of a performance statistic object are sent to the server .
Configuring Syslog Monitoring	(Optional) It is used to configure parameters of the syslog monitoring function .	
	logging userinfo	Enables logging of login/exit attempts.
	logging userinfo command-log	Enables logging of operations.
Synchronizing User Input with Log Output	(Optional) It is used to synchronize the user input with log output.	
	logging synchronous	Synchronizes user input with log output.

8.4.1 Configuring Syslog Format

Configuration Effect

- Configure the format of syslogs.

Notes

RFC3164 Log Format

- If the device does not have the real time clock (RTC), which is used to record the system absolute time, the device uses its startup time (uptime) as the syslog timestamp by default. If the device has the RTC, the device uses its absolute time (datetime) as the syslog timestamp by default.
- The log sequence number is a 6-digit integer. Each time a log is generated, the sequence number increases by one. Each time the sequence number increases from 000000 to 1,000,000, or reaches 2^32, the sequence number starts from 000000 again.

RFC5424 Log Format

- After the RFC5424 log format is enabled, the timestamp is uniform.
- In the RFC5424 log format, the timestamp may or may not contain the time zone. Currently, only the timestamp without the time zone is supported.

Configuration Steps

Configuring the Timestamp Format of Syslogs

- (Optional) By default, the datetime timestamp format is used.
- Unless otherwise specified, perform this configuration on the device to configure the timestamp format.

Adding the Sysname to the Syslog

- (Optional) By default, the syslog does not contain the sysname.
- Unless otherwise specified, perform this configuration on the device to add the sysname to the syslog.

Adding the Sequence Number to the Syslog

- (Optional) By default, the syslog does not contain the sequence number.
- Unless otherwise specified, perform this configuration on the device to add the sequence number to the syslog.

Enabling the Standard Log Format

- (Optional) By default, the default log format is used.
- Unless otherwise specified, perform this configuration on the device to enable the standard log format.

Enabling the Private Log Format

- (Optional) By default, the default log format is used.
- Unless otherwise specified, perform this configuration on the device to enable the private log format.

Enabling the RFC5424 Log Format

- (Optional) By default, the RFC5424 log format is disabled.
- Unless otherwise specified, perform this configuration on the device to enable the RFC5424 log format.

Verification

- Generate a syslog, and check the log format.

Related Commands

Configuring the Timestamp Format of Syslogs

Command	**service timestamps** [*message-type* [**uptime** | **datetime** [**msec**] [**year**]]]
Parameter Description	*message-type*: Indicates the log type. There are two log types: log and debug. **uptime**: Indicates the device startup time in the format of dd:hh:mm:ss, for example, 07:00:10:41. **datetime**: Indicates the current device time in the format of MM DD hh:mm:ss, for example, Jul 27 16:53:07. **msec**: Indicates that the current device time contains millisecond.

	year: Indicates that the current device time contains year.
Command Mode	Global configuration mode
Configuration Usage	Two syslog timestamp formats are available, namely, uptime and datetime. You can select a timestamp format as required.

Adding the Sysname to the Syslog

Command	**service sysname**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	This command is used to add the sysname to the log to enable you to learn about the device that sends syslogs to the server.

Adding the Sequence Number to the Syslog

Command	**service sequence-numbers**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	This command is used to add the sequence number to the log. The sequence number starts from 1. After the sequence number is added, you can learn clearly whether any log is lost and the generation sequence of logs.

Enabling the Standard Syslog Format

Command	**service standard-syslog**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	By default, logs are displayed in the following format (default format): *timestamp: %module-level-mnemonic: content If the standard syslog format is enabled, logs are displayed in the following format: timestamp %module-level-mnemonic: content Compared with the default format, an asterisk (*) is missing in front of the timestamp, and a colon (:) is missing at the end of the timestamp in the standard log format.

Enabling the Private Syslog Format

Command	**service private-syslog**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	By default, logs are displayed in the following format (default format): *timestamp: %module-level-mnemonic: content If the private syslog format is enabled, logs are displayed in the following format: timestamp module-level-mnemonic: content Compared with the default format, an asterisk (*) is missing in front of the timestamp, a colon (:) is missing at the end of the timestamp, and a percent sign (%) is missing in front of the module name in the private log format.

Enabling the RFC5424 Syslog Format

Command	**service log-format rfc5424**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	After the new format (RFC5424 log format) is enabled, the **service sequence-numbers**, **service sysname**, **service timestamps**, **service private-syslog**, and **service standard-syslog** commands that are applicable only to the old format (RFC3164 log format) loss effect and are hidden. After the old format (RFC3164 log format) is enabled, the **logging delay-send**, **logging policy**, and **logging statistic** commands that are applicable only to the RFC5424 log format loss effect and are hidden. After log format switchover, the outputs of the **show logging** and **show logging config** commands change accordingly.

Configuration Example

Enabling the RFC3164 Log Format

Scenario	It is required to configure the timestamp format as follows: 1. Enable the RFC3164 format. 2. Change the timestamp format to datetime and add the millisecond and year to the timestamp. 3. Add the sysname to the log. 4. Add the sequence number to the log.
Configuration Steps	● Configure the syslog format.
	FS# configure terminal

	FS(config)# no service log-format rfc5424 FS(config)# service timestamps log datetime year msec FS(config)# service timestamps debug datetime year msec FS(config)# service sysname FS(config)# service sequence-numbers
Verification	After the timestamp format is configured, verify that new syslogs are displayed in the RFC3164 format. ● Run the **show logging config** command to display the configuration. ● Enter or exit global configuration mode to generate a new log, and check the format of the timestamp in the new log.
	FS(config)#exit 001302: *Jun 14 2013 19:01:40.293: FS%SYS-5-CONFIG_I: Configured from console by admin on console FS#show logging config Syslog logging: enabled Console logging: level informational, 1306 messages logged Monitor logging: level informational, 0 messages logged Buffer logging: level informational, 1306 messages logged File logging: level informational, 121 messages logged File name:syslog_test.txt, size 128 Kbytes, have written 5 files Standard format:false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable Count log messages: enable Trap logging: level informational, 121 message lines logged,0 fail

Enabling the RFC5424 Log Format

Scenario	It is required to enable the RFC5424 format.
Configuration Steps	● Configure the syslog format.
	FS# configure terminal FS(config)# service log-format rfc5424
Verification	Verify that new syslogs are displayed in the RFC5424 format.

	● Run the **show logging config** command to display the configuration. ● Enter or exit global configuration mode to generate a new log, and check the format of the new log.
	FS(config)#exit <133>1 2013-07-24T12:19:33.130290Z FSSYS 5 CONFIG - Configured from console by console FS#show logging config Syslog logging: enabled Console logging: level debugging, 4740 messages logged Monitor logging: level debugging, 0 messages logged Buffer logging: level debugging, 4745 messages logged Statistic log messages: disable Statistic log messages to terminal: disable Delay-send file name:syslog_ftp_server, Current write index:3, Current send index:3, Cycle:10 seconds Count log messages: enable Trap logging: level informational, 2641 message lines logged,4155 fail logging to 192.168.23.89 logging to 2000::1 Delay-send logging: 2641 message lines logged logging to 192.168.23.89 by tftp

8.4.2 Sending Syslogs to the Console

Configuration Effect

- Send syslogs to the Console to facilitate the administrator to monitor the performance of the system.

Notes

- If too many syslogs are generated, you can limit the log rate to reduce the number of logs displayed on the Console.

Configuration Steps

Enabling Logging

- (Optional) By default, the logging function is enabled.

Enabling Log Statistics

- (Optional) By default, log statistics is disabled.
- Unless otherwise specified, perform this configuration on the device to enable log statistics.

Configuring the Level of Logs Displayed on the Console

- (Optional) By default, the level of logs displayed on the Console is debugging (Level 7).

- Unless otherwise specified, perform this configuration on the device to configure the level of logs displayed on the Console.

Configuring the Log Rate Limit

- (Optional) By default, the no rate limit is configured.
- Unless otherwise specified, perform this configuration on the device to limit the log rate.

Verification

- Run the show logging config command to display the level of logs displayed on the Console.

Related Commands

Enabling Logging

Command	**logging on**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	By default, logging is enabled. Do not disable logging in general cases. If too many syslogs are generated, you can configure log levels to reduce the number of logs.

Enabling Log Statistics

Command	**logging count**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	By default, log statistics is disabled. If log statistics is enabled, syslogs will be classified and counted. The system records the number of times a log is generated and the last time when the log is generated.

Configuring the Level of Logs Displayed on the Console

Command	**logging console** [*level*]
Parameter Description	*level*: Indicates the log level.
Command Mode	Global configuration mode
Configuration Usage	By default, the level of logs displayed on the Console is debugging (Level 7). You can run the **show logging config** command in privileged EXEC mode to display the level of logs displayed on the Console.

Configuring the Log Rate Limit

Command	**logging rate-limit** { *number* | **all** *number* | **console** {*number* | **all** *number*} } [**except** [*severity*]]
Parameter Description	*number*: Indicates the maximum number of logs processed per second. The value ranges from 1 to 10,000. **all**: Indicates that rate limit is applied to all logs ranging from Level 0 to Level 7. **console**: Indicates the number of logs displayed on the Console per second. **except** *severity*: Rate limit is not applied to logs with a level equaling to or lower than the specified severity level. By default, the severity level is error (Level 3), that is, rate limit is not applied to logs of Level 3 or lower.
Command Mode	Global configuration mode
Configuration Usage	By default, no rate limit is configured.

Configuration Example

Sending Syslogs to the Console

Scenario	It is required to configure the function of displaying syslogs on the Console as follows: 1. Enable log statistics. 2. Set the level of logs that can be displayed on the Console to informational (Level 6). 3. Set the log rate limit to 50.
Configuration Steps	● Configure parameters for displaying syslogs on the Console.
	FS# configure terminal FS(config)# logging count FS(config)# logging console informational FS(config)# logging rate-limit console 50
Verification	● Run the **show logging config** command to display the configuration.
	FS(config)#show logging config Syslog logging: enabled Console logging: level informational, 1303 messages logged Monitor logging: level debugging, 0 messages logged Buffer logging: level debugging, 1303 messages logged File logging: level informational, 118 messages logged File name:syslog_test.txt, size 128 Kbytes, have written 5 files Standard format:false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable

Scenario	It is required to configure the function of displaying syslogs on the Console as follows: 1. Enable log statistics. 2. Set the level of logs that can be displayed on the Console to informational (Level 6). 3. Set the log rate limit to 50.
Configuration Steps	● Configure parameters for displaying syslogs on the Console.
	FS# configure terminal FS(config)# logging count FS(config)# logging console informational FS(config)# logging rate-limit console 50
Verification	● Run the **show logging config** command to display the configuration.
	Sysname log messages: enable Count log messages: enable Trap logging: level informational, 118 message lines logged,0 fail

8.4.3 Sending Syslogs to the Monitor Terminal

Configuration Effect

- Send syslogs to a remote monitor terminal to facilitate the administrator to monitor the performance of the system.

Notes

- If too many syslogs are generated, you can limit the log rate to reduce the number of logs displayed on the monitor terminal.
- By default, the current monitor terminal is not allowed to display logs after you access the device remotely. You need to manually run the terminal monitor command to allow the current monitor terminal to display logs.

Configuration Steps

Allowing the Monitor Terminal to Display Logs

- (Mandatory) By default, the monitor terminal is not allowed to display logs.
- Unless otherwise specified, perform this operation on every monitor terminal connected to the device.

Configuring the Level of Logs Displayed on the Monitor Terminal

- (Optional) By default, the level of logs displayed on the monitor terminal is debugging (Level 7).
- Unless otherwise specified, perform this configuration on the device to configure the level of logs displayed on the monitor terminal.

Verification

- Run the show logging config command to display the level of logs displayed on the monitor terminal.

Related Commands

Allowing the Monitor Terminal to Display Logs

Command	**terminal monitor**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Configuration Usage	By default, the current monitor terminal is not allowed to display logs after you access the device remotely. You need to manually run the **terminal monitor** command to allow the current monitor terminal to display logs.

Configuring the Level of Logs Displayed on the Monitor Terminal

Command	**logging monitor** [*level*]
Parameter Description	*level*: Indicates the log level.
Command Mode	Global configuration mode
Configuration Usage	By default, the level of logs displayed on the monitor terminal is debugging (Level 7). You can run the **show logging config** command in privileged EXEC mode to display the level of logs displayed on the monitor terminal.

Configuration Example

Sending Syslogs to the Monitor Terminal

Scenario	It is required to configure the function of displaying syslogs on the monitor terminal as follows: 1. Display logs on the monitor terminal. 2. Set the level of logs that can be displayed on the monitor terminal to informational (Level 6).
Configuration Steps	● Configure parameters for displaying syslogs on the monitor terminal.
	FS# configure terminal FS(config)# logging monitor informational FS(config)# line vty 0 4 FS(config-line)# monitor
Verification	● Run the **show logging config** command to display the configuration.
	FS#show logging config Syslog logging: enabled Console logging: level informational, 1304 messages logged

Scenario	It is required to configure the function of displaying syslogs on the monitor terminal as follows: 1. Display logs on the monitor terminal. 2. Set the level of logs that can be displayed on the monitor terminal to informational (Level 6).
Configuration Steps	● Configure parameters for displaying syslogs on the monitor terminal.
	FS# configure terminal FS(config)# logging monitor informational FS(config)# line vty 0 4 FS(config-line)# monitor
Verification	● Run the **show logging config** command to display the configuration.
	Monitor logging: level informational, 0 messages logged Buffer logging: level debugging, 1304 messages logged File logging: level informational, 119 messages logged File name:syslog_test.txt, size 128 Kbytes, have written 5 files Standard format:false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable Count log messages: enable Trap logging: level informational, 119 message lines logged,0 fail

Common Errors

- To disable this function, run the terminal no monitor command, instead of the no terminal monitor command.

8.4.4 Writing Syslogs into the Memory Buffer

Configuration Effect

- Write syslogs into the memory buffer so that the administrator can view recent syslogs by running the show logging command.

Notes

- If the buffer is full, old logs will be overwritten by new logs that are written into the memory buffer.

Configuration Steps

↘ Writing Logs into the Memory Buffer

- (Optional) By default, the system writes logs into the memory buffer, and the default level of logs is debugging (Level 7).

- Unless otherwise specified, perform this configuration on the device to write logs into the memory buffer.

Verification

- Run the show logging config command to display the level of logs written into the memory buffer.
- Run the show logging command to display the level of logs written into the memory buffer.

Related Commands

Writing Logs into the Memory Buffer

Command	**logging buffered** [*buffer-size*] [*level*]
Parameter Description	*buffer-size*: Indicates the size of the memory buffer. *level*: Indicates the level of logs that can be written into the memory buffer.
Command Mode	Global configuration mode
Configuration Usage	By default, the level of logs written into the memory buffer is debugging (Level 7). Run the **show logging** command in privileged EXEC mode to display the level of logs written into the memory buffer and the buffer size.

Configuration Example

Writing Syslogs into the Memory Buffer

Scenario	It is required to configure the function of writing syslogs into the memory buffer as follows: 1. Set the log buffer size to 128 KB (131,072 bytes). 2. Set the information level of logs that can be written into the memory buffer to informational (Level 6).
Configuration Steps	• Configure parameters for writing syslogs into the memory buffer.
	FS# configure terminal FS(config)# logging buffered 131072 informational
Verification	• Run the **show logging config** command to display the configuration and recent syslogs.
	FS#show logging Syslog logging: enabled Console logging: level informational, 1306 messages logged Monitor logging: level informational, 0 messages logged Buffer logging: level informational, 1306 messages logged File logging: level informational, 121 messages logged File name:syslog_test.txt, size 128 Kbytes, have written 5 files Standard format:false

Scenario	It is required to configure the function of writing syslogs into the memory buffer as follows: 1. Set the log buffer size to 128 KB (131,072 bytes). 2. Set the information level of logs that can be written into the memory buffer to informational (Level 6).
Configuration Steps	● Configure parameters for writing syslogs into the memory buffer.
	FS# configure terminal FS(config)# logging buffered 131072 informational
Verification	● Run the **show logging config** command to display the configuration and recent syslogs.
	Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable Count log messages: enable Trap logging: level informational, 121 message lines logged,0 fail Log Buffer (Total 131072 Bytes): have written 4200 001301: *Jun 14 2013 19:01:09.488: FS%SYS-5-CONFIG_I: Configured from console by admin on console 001302: *Jun 14 2013 19:01:40.293: FS%SYS-5-CONFIG_I: Configured from console by admin on console //Logs displayed are subject to the actual output of the **show logging** command.

8.4.5 Sending Syslogs to the Log Server

Configuration Effect

- Send syslogs to the log server to facilitate the administrator to monitor logs on the server.

Notes

- If the device has a MGMT interface and is connected to the log server through the MGMT interface, you must add the oob option (indicating that syslogs are sent to the log server through the MGMT interface) when configuring the logging server command.
- To send logs to the log server, you must add the timestamp and sequence number to logs. Otherwise, the logs are not sent to the log server.

Configuration Steps

Sending Logs to a Specified Log Server

- (Mandatory) By default, syslogs are not sent to any log server.
- Unless otherwise specified, perform this configuration on every device.

Configuring the Level of Logs Sent to the Log Server

- (Optional) By default, the level of logs sent to the log server is informational (Level 6).

- Unless otherwise specified, perform this configuration on the device to configure the level of logs sent to the log server.

Configuring the Facility Value of Logs Sent to the Log Server

- (Optional) If the RFC5424 format is disabled, the facility value of logs sent to the log server is local7 (23) by default. If the RFC5424 format is enabled, the facility value of logs sent to the log server is local0 (16) by default.
- Unless otherwise specified, perform this configuration on the device to configure the facility value of logs sent to the log server.

Configuring the Source Interface of Logs Sent to the Log Server

- (Optional) By default, the source interface of logs sent to the log server is the interface sending the logs.
- Unless otherwise specified, perform this configuration on the device to configure the source interface of logs sent to the log server.

Configuring the Source Address of Logs Sent to the Log Server

- (Optional) By default, the source address of logs sent to the log server is the IP address of the interface sending the logs.
- Unless otherwise specified, perform this configuration on the device to configure the source address of logs sent to the log server.

Verification

- Run the show logging config command to display the configurations related to the log server.

Related Commands

Sending Logs to a Specified Log Server

Command	**logging server** [**oob**] { *ip-address* } [**udp-port** *port*] Or **logging** { *ip-address* } [**udp-prot** *port*]
Parameter Description	**oob**: Indicates that logs are sent to the log server through the MGMT interface. *ip-address*: Specifies the IP address of the host that receives logs. **udp-port** *port*: Specifies the port ID of the log server. The default port ID is 514.
Command Mode	Global configuration mode
Configuration Usage	This command is used to specify the address of the log server that receives logs. You can specify multiple log servers, and logs will be sent simultaneously to all these log servers. You can configure up to five log servers on a FSproduct.

Configuring the Level of Logs Sent to the Log Server

Command	**logging trap** [*level*]
Parameter Description	*level*: Indicates the log level.
Command Mode	Global configuration mode
Configuration	By default, the level of logs sent to the log server is informational (Level 6). You can run the **show logging config** command in privileged EXEC mode to display the level of logs sent to the log

Usage	server.

Configuring the Facility Value of Logs Sent to the Log Server

Command	**logging facility** *facility-type*
Parameter Description	*facility-type*: Indicates the facility value of logs.
Command Mode	Global configuration mode
Configuration Usage	If the RFC5424 format is disabled, the facility value of logs sent to the server is local7 (23) by default. If the RFC5424 format is enabled, the facility value of logs sent to the server is local0 (16) by default.

Configuring the Source Interface of Logs Sent to the Log Server

Command	**logging source** [**interface**] *interface-type interface-number*
Parameter Description	*interface-type*: Indicates the interface type. *interface-number*: Indicates the interface number.
Command Mode	Global configuration mode
Configuration Usage	By default, the source interface of logs sent to the log server is the interface sending the logs. To facilitate management, you can use this command to set the source interface of all logs to an interface so that the administrator can identify the device that sends the logs based on the unique address.

Configuring the Source Address of Logs Sent to the Log Server

Command	**logging source** { **ip** *ip-address* }
Parameter Description	**ip** *ip-address*: Specifies the source IPv4 address of logs sent to the IPv4 log server.
Command Mode	Global configuration mode
Configuration Usage	By default, the source IP address of logs sent to the log server is the IP address of the interface sending the logs. To facilitate management, you can use this command to set the source IP address of all logs to the IP address of an interface so that the administrator can identify the device that sends the logs based on the unique address..

Configuration Example

Sending Syslogs to the Log Server

Scenario	It is required to configure the function of sending syslogs to the log server as follows: 1. Set the IPv4 address of the log server to 10.1.1.100. 2. Set the level of logs that can be sent to the log server to debugging (Level 7). 3. Set the source interface to Loopback 0.

Configuration Steps	● Configure parameters for sending syslogs to the log server.
	FS# configure terminal FS(config)# logging server 10.1.1.100 FS(config)# logging trap debugging FS(config)# logging source interface Loopback 0
Verification	● Run the **show logging config** command to display the configuration.
	FS#show logging config Syslog logging: enabled Console logging: level informational, 1307 messages logged Monitor logging: level informational, 0 messages logged Buffer logging: level informational, 1307 messages logged File logging: level informational, 122 messages logged File name:syslog_test.txt, size 128 Kbytes, have written 5 files Standard format:false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable Count log messages: enable Trap logging: level debugging, 122 message lines logged,0 fail logging to 10.1.1.100

8.4.6 Writing Syslogs into Log Files

Configuration Effect

- Write syslogs into log files at the specified interval so that the administrator can view history logs anytime on the local device.

Notes

- Sylsogs are not immediately written into log files. They are first buffered in the memory buffer, and then written into log files either periodically (at the interval of one hour by default) or when the buffer is full.

Configuration Steps

Writing Logs into Log Files

- (Mandatory) By default, syslogs are not written to any log file.
- Unless otherwise specified, perform this configuration on every device.

Configuring the Number of Log Files

- (Optional) By default, syslogs are written to 16 log files.
- Unless otherwise specified, perform this configuration on the device to configure the number of files which logs are written into.

Configuring the Interval at Which Logs Are Written into Log Files

- (Optional) By default, syslogs are written to log files every hour.
- Unless otherwise specified, perform this configuration on the device to configure the interval at which logs are written into log files.

Configuring the Storage Time of Log Files

- (Optional) By default, no storage time is configured.
- Unless otherwise specified, perform this configuration on the device to configure the storage time of log files.

Immediately Writing Logs in the Buffer into Log Files

- (Optional) By default, syslogs are stored in the buffer and then written into log files periodically or when the buffer is full.
- Unless otherwise specified, perform this configuration to write logs in the buffer into log files immediately. This command takes effect only once after it is configured.

Verification

- Run the show logging config command to display the configurations related to the log server.

Related Commands

Writing Logs into Log Files

Command	**logging file** { **sata0:***filename* | **flash:***filename* | **usb0**:*filename* | **usb1**:*filename* } [*max-file-size*] [*level*]
Parameter Description	**sata0**: Indicates that log files will be stored on the hard disk. **flash**: Indicates that log files will be stored on the extended Flash. **usb0**: Indicates that log files will be stored on USB 0. This option is supported only when the device has one USB port and a USB flash drive is inserted into the USB port. **usb1**: Indicates that log files will be stored on USB 1. This option is supported only when the device has two USB ports and USB flash drives are inserted into the USB ports. *filename*: Indicates the log file name, which does not contain a file name extension. The file name extension is always txt. *max-file-size*: Indicates the maximum size of a log file. The value ranges from 128 KB to 6 MB. The default value is 128 KB. *level*: Indicates the level of logs that can be written into a log file.
Command Mode	Global configuration mode

Configuration Usage	This command is used to create a log file with the specified file name on the specified file storage device. The file size increases with the amount of logs, but cannot exceed the configured maximum size. If not specified, the maximum size of a log file is 128 KB by default. After this command is configured, the system saves logs to log files. A log file name does not contain any file name extension. The file name extension is always txt, which cannot be changed. After this command is configured, logs will be written into log files every hour. If you run the **logging flie flash:syslog** command, a total of 16 log files will be created, namely, **syslog.txt**, **syslog_1.txt**, **syslog_2.txt**, …, **syslog_14.txt**, and **syslog_15.txt**. Logs are written into the 16 log files in sequence. For example, the system writes logs into **syslog_1.txt** after **syslog.txt** is full. When **syslog_15.txt** is full, logs are written into **syslog.txt** again,

Configuring the Number of Log Files

Command	**logging file numbers** *numbers*
Parameter Description	*numbers*: Indicates the number of log files. The value ranges from 2 to 32.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the number of log files. If the number of log files is modified, the system will not delete the log files that have been generated. Therefore, you need to manually delete the existing log files to save the space of the extended flash. (Before deleting existing log files, you can transfer these log files to an external server through TFTP.) For example, after the function of writing logs into log files is enabled, 16 log files will be created by default. If the device has generated 16 log files and you change the number of log files to 2, new logs will be written into **syslog.txt** and **syslog_1.txt** by turns. The existing log files from **syslog_2.txt** to **syslog_15.txt** will be preserved. You can manually delete these log files.

Configuring the Interval at Which Logs Are Written into Log Files

Command	**logging flash interval** *seconds*
Parameter Description	*seconds*: Indicates the interval at which logs are written into log files. The value ranges from 1s to 51,840s.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the interval at which logs are written into log files. The countdown starts after the command is configured.

Configuring the Storage Time of Log Files

Command	**logging life-time level** *level days*
Parameter Description	*level*: Indicates the log level. *days*: Indicates the storage time of log files. The unit is day. The storage time is not less than seven days.
Command Mode	Global configuration mode

Configuration Usage	After the log storage time is configured, the system writes logs of the same level that are generated in the same day into the same log file. The log file is named **yyyy-mm-dd_filename_level.txt**, where **yyyy-mm-dd** is the absolute time of the day when the logs are generated, **filename** is the log file named configured by the **logging file flash** command, and **level** is the log level. After you specify the storage time for logs of a certain level, the system deletes the logs after the storage time expires. Currently, the storage time ranges from 7days to 365 days. If the log storage time is not configured, logs are stored based on the file size to ensure compatibility with old configuration commands.

Immediately Writing Logs in the Buffer into Log Files

Command	**logging flash flush**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	After this command is configured, syslogs are stored in the buffer and then written into log files periodically or when the buffer is full. You can run this command to immediately write logs into log files. The **logging flash flush** command takes effect once after it is configured. That is, after this command is configured, logs in the buffer are immediately written to log files.

Configuration Example

Writing Syslogs into Log Files

Scenario	It is required to configure the function of writing syslogs into log files as follows: 1. Set the log file name to syslog. 2. Set the level of logs sent to the Console to debugging (Level 7). 3. Set the interval at which device logs are written into files to 10 minutes (600s).
Configuration Steps	● Configure parameters for writing syslogs into log files.
	FS# configure terminal FS(config)# logging file flash:syslog debugging FS(config)# logging flash interval 600
Verification	● Run the **show logging config** command to display the configuration.
	FS(config)#show logging config Syslog logging: enabled Console logging: level informational, 1307 messages logged Monitor logging: level informational, 0 messages logged

Scenario	It is required to configure the function of writing syslogs into log files as follows: 1. Set the log file name to syslog. 2. Set the level of logs sent to the Console to debugging (Level 7). 3. Set the interval at which device logs are written into files to 10 minutes (600s).
Configuration Steps	● Configure parameters for writing syslogs into log files.
	FS# configure terminal FS(config)# logging file flash:syslog debugging FS(config)# logging flash interval 600
Verification	● Run the **show logging config** command to display the configuration.
	Buffer logging: level informational, 1307 messages logged File logging: level debugging, 122 messages logged File name:syslog.txt, size 128 Kbytes, have written 1 files Standard format:false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable Count log messages: enable Trap logging: level debugging, 122 message lines logged,0 fail logging to 10.1.1.100

8.4.7 Configuring Syslog Filtering

Configuration Effect

- Filter out a specified type of syslogs if the administrator does not want to display these syslogs.
- By default, logs generated by all modules are displayed on the Console or other terminals. You can configure log filtering rules to display only desired logs.

Notes

- Two filtering modes are available: contains-only and filter-only. You can configure only one filtering mode at a time.
- If the same module, level, or mnemonic is configured in both the single-match and exact-match rules, the single-match rule prevails over the exact-match rule.

Configuration Steps

Configuring the Log Filtering Direction

- (Optional) By default, the filtering direction is all, that is, all logs are filtered out.
- Unless otherwise specified, perform this configuration on the device to configure the log filtering direction.

Configuring the Log Filtering Mode

- (Optional) By default, the log filtering mode is filter-only.
- Unless otherwise specified, perform this configuration on the device to configure the log filtering mode.

Configuring the Log Filtering Rule

- (Mandatory) By default, no filtering rule is configured.
- Unless otherwise specified, perform this configuration on the device to configure the log filtering rule.

Verification

- Run the show running command to display the configuration.

Related Commands

Configuring the Log Filtering Direction

Command	**logging filter direction** { **all** | **buffer** | **file** | **server** | **terminal** }
Parameter Description	**all**: Filters out all logs. **buffer**: Filters out logs sent to the log buffer, that is, the logs displayed by the **show logging** command. **file**: Filters out logs written into log files. **server**: Filters out logs sent to the log server. **terminal**: Filters out logs sent to the Console and VTY terminal (including Telnet and SSH).
Command Mode	Global configuration mode
Configuration Usage	The default filtering direction is **all**, that is, all logs are filtered out. Run the **default logging filter direction** command to restore the default filtering direction.

Configuring the Log Filtering Mode

Command	**logging filter type** { **contains-only** | **filter-only** }
Parameter Description	**contains-only**: Indicates that only logs that contain keywords specified in the filtering rules are displayed. **filter-only**: Indicates that logs that contain keywords specified in the filtering rules are filtered out and will not be displayed.
Command Mode	Global configuration mode
Configuration Usage	Log filtering modes include contains-only and filter-only. The default filtering mode is filter-only.

Configuring the Log Filtering Rule

Command	**logging filter rule** { **exact-match module** *module-name* **mnemonic** *mnemonic-name* **level** *level* | **single-match** { **level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name* } }
Parameter Description	**exact-match**: If exact-match is selected, you must specify all three filtering options. **single-match**: If single-match is selected, you may specify only one of the three filtering options. **module** *module-name*: Indicates the module name. Logs of this module will be filtered out. **mnemonic** *mnemonic-name*: Indicates the mnemonic. Logs with this mnemonic will be filtered out. **level** *level*: Indicates the log level. Logs of this level will be filtered out.
Command Mode	Global configuration mode
Configuration Usage	Log filtering rules include exact-match and single-match. The **no logging filter rule exact-match** [**module** *module-name* **mnemonic** *mnemonic-name* **level** *level*] command is used to delete the exact-match filtering rules. You can delete all exact-match filtering rules at a time or one by one. The **no logging filter rule single-match** [**level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name*] command is used to delete the single-match filtering rules. You can delete all single-match filtering rules at a time or one by one.

Configuration Example

Configuring Syslog Filtering

Scenario	It is required to configure the syslog filtering function as follows: 1. Set the filtering directions of logs to **terminal** and **server.** 2. Set the log filtering mode to filter-only. 3. Set the log filtering rule to single-match to filter out logs that contain the module name "SYS".
Configuration Steps	● Configure the syslog filtering function.
	FS# configure terminal FS(config)# logging filter direction server FS(config)# logging filter direction terminal FS(config)# logging filter type filter-only FS(config)# logging filter rule single-match module SYS
Verification	● Run the **show running-config | include loggging** command to display the configuration. ● Enter and exit global configuration mode, and verify that the system displays logs accordingly.
	FS#configure Enter configuration commands, one per line. End with CNTL/Z. FS(config)#exit FS# FS#show running-config | include logging logging filter direction server

Scenario	It is required to configure the syslog filtering function as follows: 1. Set the filtering directions of logs to **terminal** and **server.** 2. Set the log filtering mode to filter-only. 3. Set the log filtering rule to single-match to filter out logs that contain the module name "SYS".
Configuration Steps	● Configure the syslog filtering function.
	FS# configure terminal FS(config)# logging filter direction server FS(config)# logging filter direction terminal FS(config)# logging filter type filter-only FS(config)# logging filter rule single-match module SYS
Verification	● Run the **show running-config | include loggging** command to display the configuration. ● Enter and exit global configuration mode, and verify that the system displays logs accordingly.
	logging filter direction terminal logging filter rule single-match module SYS

8.4.8 Configuring Level-based Logging

Configuration Effect

- You can use the level-based logging function to send syslogs to different destinations based on different module and severity level. For example, you can configure a command to send WLAN module logs of Level 4 or lower to the log server, and WLAN module logs of Level 5 or higher to local log files.

Notes

- Level-based logging takes effect only when the RFC5424 format is enabled.

Configuration Steps

Configuring Level-based Logging

- (Optional) By default, logs are sent in all directions.
- Unless otherwise specified, perform this configuration on the device to configure logging polices to send syslogs to different destinations based on module and severity level.

Verification

- Run the show running command to display the configuration.

Related Commands

Configuring Level-based Logging

Command	**logging policy module** *module-name* [**not-lesser-than**] *level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** }
Parameter Description	*module-name*: Indicates the name of the module to which the logging policy is applied. **not-lesser-than**: If this option is specified, logs of the specified level or higher will be sent to the specified destination, and other logs will be filtered out. If this option is not specified, logs of the specified level or lower will be sent to the specified destination, and other logs will be filtered out. *level*: Indicates the level of logs for which the logging policy is configured. **all**: Indicates that the logging policy is applied to all logs. **server**: Indicates that the logging policy is applied only to logs sent to the log server. **file**: Indicates that the logging policy is applied only to logs written into log files. **console**: Indicates that the logging policy is applied only to logs sent to the Console. **monitor**: Indicates that the logging policy is applied only to logs sent to a remote terminal. **buffer**: Indicates that the logging policy is applied only to logs stored in the buffer.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure logging polices to send syslogs to different destinations based on module and severity level.

Configuration Example

Configuring Level-based Logging

Scenario	It is required to configure the logging policies as follows: 1. Send logs of Level 5 or higher that are generated by the system to the Console. 2. Send logs of Level 3 or lower that are generated by the system to the buffer.
Configuration Steps	● Configure the logging policies.
	FS# configure terminal FS(config)# logging policy module SYS not-lesser-than 5 direction console FS(config)# logging policy module SYS 3 direction buffer
Verification	● Run the **show running-config | include logging policy** command to display the configuration. ● Exit and enter global configuration mode to generate a log containing module name "SYS". Verify that the log is sent to the destination as configured.
	FS#show running-config | include logging policy logging policy module SYS not-lesser-than 5 direction console logging policy module SYS 3 direction buffer

8.4.9 Configuring Delayed Logging

Configuration Effect

- By default, delayed logging is enabled by default at the interval of 3600s (one hour). The name of the log file sent to the remote server is File size_Device IP address_Index.txt. Logs are not sent to the Console or remote terminal.
- You can configure the interval based on the frequency that the device generates logs for delayed uploading. This can reduce the burden on the device, syslog server, and network. In addition, you can configure the name of the log file as required.

Notes

- This function takes effect only when the RFC5424 format is enabled.
- It is recommended to disable the delayed display of logs on the Console and remote terminal. Otherwise, a large amount of logs will be displayed, increasing the burden on the device.
- The file name cannot contain any dot (.) because the system automatically adds the index and the file name extension (.txt) to the file name when generating a locally buffered file. The index increases each time a new file is generated. In addition, the file name cannot contain characters prohibited by your file system, such as \, /, :, *, ", <, >, and |. For example, the file name is log_server, the current file index is 5, the file size is 1000 bytes, and the source IP address is 10.2.3.5.The name of the log file sent to the remote server is log_server_1000_10.2.3.5_5.txt while the name of the log file stored on the device is log_server_5.txt.
- If few logs are generated, you can set the interval to a large value so that many logs can be sent to the remote server at a time.

Configuration Steps

Enabling Delayed Display of Logs on Console and Remote Terminal

- (Optional) By default, delayed display of logs on the Console and remote terminal is disabled.
- Unless otherwise specified, perform this configuration on the device to enable delayed display of logs on the Console and remote terminal.

Configuring the Name of the File for Delayed Logging

- (Optional) By default, the name of the file for delayed logging is File size_Device IP address_Index.txt.
- Unless otherwise specified, perform this configuration on the device to configure the name of the file for delayed logging.

Configuring the Delayed Logging Interval

- (Optional) By default, the delayed logging interval is 3600s (one hour).
- Unless otherwise specified, perform this configuration on the device to configure the delayed logging interval.

Configuring the Server Address and Delayed Logging Mode

- (Optional) By default, log files are not sent to any remote server.
- Unless otherwise specified, perform this configuration on the device to configure the server address and delayed logging mode

Verification

- Run the show running command to display the configuration.

Related Commands

Enabling Delayed Display of Logs on Console and Remote Terminal

Command	**logging delay-send terminal**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	N/A.

Configuring the Name of the File for Delayed Logging

Command	**logging delay-send file flash:***filename*
Parameter Description	**flash:***filename*: Indicates the name of the file on the local device where logs are buffered.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the name of the file on the local device where logs are buffered. The file name cannot contain any dot (.) because the system automatically adds the index and the file name extension (.txt) to the file name when generating a locally buffered file. The index increases each time a new file is generated. In addition, the file name cannot contain characters prohibited by your file system, such as \, /, :, *, ", <, >, and |. For example, the configured file name is log_server, the current file index is 5, the file size is 1000 bytes, and the source IP address is 10.2.3.5. The name of the log file sent to the remote server is **log_server_1000_10.2.3.5_5.txt** while the name of the log file stored on the device is **log_server_5.txt**.

Configuring the Delayed Logging Interval

Command	**logging delay-send interval** *seconds*
Parameter Description	*seconds*: Indicates the delayed logging interval. The unit is second.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the delayed logging interval. The value ranges from 600s to 65,535s.

Configuring the Server Address and Delayed Logging Mode

Command	**logging delay-send server** { [**oob**] *ip-address* } **mode** { **ftp user** *username* **password** [**0** | **7**] *password* | **tftp** }
Parameter	**oob**: Indicates that logs are sent to the server through the MGMT port of the device, that is, by means of out-band

Description	communication. *ip-address*: Indicates the IP address of the server that receives logs. *username*: Specifies the user name of the FTP server. *password*: Specifies the password of the FTP server. **0**: (Optional) Indicates that the following password is in plain text. **7**: Indicates that the following password is encrypted.
Command Mode	Global configuration mode
Configuration Usage	This command is used to specify an FTP or a TFTP server for receiving the device logs. You can configure a total of five FTP or TFTP servers, but a server cannot be both an FTP and TFTP server.. Logs will be simultaneously sent to all FTP or TFTP servers.

Configuration Example

Configuring Delayed Logging

Scenario	It is required to configure the delayed logging function as follows: 1. Enable the delayed display of logs on the Console and remote terminal. 2. Set the delayed logging interval to 7200s (two hours). 3. Set the name of the file for delayed logging to syslog_FS. 4. Set the IP address of the server to 192.168.23.12, user name to admin, password to admin, and logging mode to FTP.
Configuration Steps	● Configure the delayed logging function.
	FS# configure terminal FS(config)# logging delay-send terminal FS(config)# logging delay-send interval 7200 FS(config)# logging delay-send file flash:syslog_FS FS(config)# logging delay-send server 192.168.23.12 mode ftp user admin password admin
Verification	● Run the **show running-config | include logging delay-send** command to display the configuration. ● Verify that logs are sent to the remote FTP server after the timer expires.
	FS#show running-config | include logging delay-send logging delay-send terminal logging delay-send interval 7200 logging delay-send file flash:syslog_FS logging delay-send server 192.168.23.12 mode ftp user admin password admin

8.4.10 Configuring Periodical Logging

Configuration Effect

- By default, periodical logging is disabled. Periodical logging interval is 15 minutes. Periodical display of logs on the Console and remote terminal are disabled.
- You can modify the periodical logging interval. The server will collect all performance statistic logs at the time point that is the least common multiple of the intervals of all statistic objects.

Notes

- Periodical logging takes effect only when the RFC5424 format is enabled.
- The settings of the periodical logging interval and the function of displaying logs on the Console and remote terminal take effect only when the periodical logging function is enabled.
- It is recommended to disable periodical display of logs on the Console and remote terminal. Otherwise, a large amount of performance statistic logs will be displayed, increasing the burden on the device.
- To ensure the server can collect all performance statistic logs at the same time point, the timer will be restarted when you modify the periodical logging interval of a statistic object.

Configuration Steps

Enabling Periodical Logging

- (Optional) By default, periodical logging is disabled.
- Unless otherwise specified, perform this configuration on the device to enable periodical logging.

Enabling Periodical Display of Logs on Console and Remote Terminal

- (Optional) By default, periodical display of logs on the Console and remote terminal is disabled.
- Unless otherwise specified, perform this configuration on the device to enable periodical display of logs on the Console and remote terminal.

Configuring the Periodical Logging Interval

- (Optional) By default, the periodical logging interval is 15 minutes.
- Unless otherwise specified, perform this configuration on the device to configure the interval at which logs of statistic objects are sent to the server.

Verification

- Run the show running command to display the configuration.

Related Commands

Enabling Periodical Logging

Command	**logging statistic enable**
Parameter	N/A

Description	
Command Mode	Global configuration mode
Configuration Usage	This command is used to enable periodical logging. After this function is enabled, the system outputs a series of performance statistics at a certain interval so that the log server can monitor the system performance.

Enabling Periodical Display of Logs on Console and Remote Terminal

Command	**logging statistic terminal**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuring the Periodical Logging Interval

Command	**logging statistic mnemonic** *mnemonic* **interval** *minutes*
Parameter Description	*mnemonic*: Identifies a performance statistic object. *minutes*: Indicates the periodical logging interval. The unit is minute.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the periodical logging interval for a specified performance statistic object. The interval can be set to 0, 15, 30, 60, or 120 minutes. 0 indicates that periodical logging is disabled.

Configuration Example

Configuring Periodical Logging

Scenario	It is required to configure the l periodical logging function as follows: 1. Enable the periodical logging function. 2. Enable periodical display of logs on the Console and remote terminal. 3. Set the periodical logging interval of the statistic object TUNNEL_STAT to 30 minutes.
Configuration Steps	● Configure the periodical logging function.
	FS# configure terminal FS(config)# logging statistic enable FS(config)# logging statistic terminal FS(config)# logging statistic mnemonic TUNNEL_STAT interval 30

Verification	● Run the **show running-config | include logging statistic** command to display the configuration. ● After the periodical logging timer expires, verify that logs of all performance statistic objects are generated at the time point that is the least common multiple of the intervals of all statistic objects.
	FS#show running-config | include logging statistic logging statistic enable logging statistic terminal logging statistic mnemonic TUNNEL_STAT interval 30

8.4.11 Configuring Syslog Monitoring

Configuration Effect

- Record login/exit attempts. After logging of login/exit attempts is enabled, the related logs are displayed on the device when users access the device through Telnet or SSH. This helps the administrator monitor the device connections.
- Record modification of device configurations. After logging of operations is enabled, the related logs are displayed on the device when users modify the device configurations. This helps the administrator monitor the changes in device configurations.

Notes

- If both the logging userinfo command and the logging userinfo command-log command are configured on the device, only the configuration result of the logging userinfo command-log command is displayed when you run the show running-config command.

Configuration Steps

Enabling Logging of Login/Exit Attempts

- (Optional) By default, logging of login/exit attempts is disabled.
- Unless otherwise specified, perform this configuration on every line of the device to enable logging of login/exit attempts.

Enabling logging of Operations

- (Optional) By default, logging of operations is disabled.
- Unless otherwise specified, perform this configuration on every line of the device to enable logging of operations.

Verification

- Run the show running command to display the configuration.

Related Commands

Enabling Logging of Login/Exit Attempts

Command	logging userinfo
Parameter Description	N/A

Command Mode	Global configuration mode
Configuration Usage	By default, a device does not generate related logs when users log into or exit the device.

Enabling Logging of Operations

Command	**logging userinfo command-log**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	The system generates related logs when users run configuration commands. By default, a device does not generate logs when users modify device configurations.

Configuration Example

Configuring Syslog Monitoring

Scenario	It is required to configure the syslog monitoring function as follows: 1. Enable logging of login/exit attempts. 2. Enable logging of operations.
Configuration Steps	● Configure the syslog monitoring function.
	FS# configure terminal FS(config)# logging userinfo FS(config)# logging userinfo command-log
Verification	● Run the **show running-config | include logging** command to display the configuration. ● Run a command in global configuration mode, and verify that the system generates a log.
	FS#configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#interface gigabitEthernet 0/0 *Jun 16 15:03:43: %CLI-5-EXEC_CMD: Configured from console by admin command: interface GigabitEthernet 0/0 FS#show running-config | include logging logging userinfo command-log

8.4.12 Configuring Syslog Language

Configuration Effect

- The default syslog language is English.
- The default syslog language is Chinese.

Notes

Configuring the syslog language in the global configuration mode.

Configuration Steps

Configuring Syslog Language

- (Optional) The default syslog language is English.
- (Optional) The default syslog language is Chinese.

Verification

Run the **show running** command to configure the syslog language.

Related Commands

Configuring Syslog Language

Command	**logging language** { **Chinese** | **English** }
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the syslog language.

Configuration Example

Configuring Syslog Language

Scenario	It is required to set the syslog language to English (Default: Chinese).
Configuration Steps	• Configure the syslog language in the global configuration mode.
	FS# configure terminal FS(config)# logging language English
Verification	• Run the **show running-config | in logging** command to display the configuration.
	FS#show running-config | begin line line con 0 logging language English login local

Scenario	It is required to set the syslog language to English (Default: Chinese).
Configuration Steps	● Configure the syslog language in the global configuration mode.
	FS# configure terminal FS(config)# logging language English
Verification	● Run the **show running-config | in logging** command to display the configuration.
Scenario	It is required to set the syslog language to Chinese (Default: English).
Configuration Steps	● Configure the syslog language in the global configuration mode.
	FS# configure terminal FS(config)# logging language Chinese
Verification	● Run the **show running-config | in logging** command to display the configuration.
	FS#show running-config | begin line line con 0 logging language Chinese login local

8.4.13 Synchronizing User Input with Log Output

Configuration Effect

- By default, the user input is not synchronized with the log output. After this function is enabled, the content input during log output is displayed after log output is completed, ensuring integrity and continuity of the input.

Notes

- This command is executed in line configuration mode. You need to configure this command on every line as required.

Configuration Steps

Synchronizing User Input with Log Output

- (Optional) By default, the synchronization function is disabled.
- Unless otherwise specified, perform this configuration on every line to synchronize user input with log output.

Verification

- Run the show running command to display the configuration.

Related Commands

Synchronizing User Input with Log Output

Command	**logging synchronous**
Parameter	N/A

Description	
Command Mode	Line configuration mode
Configuration Usage	This command is used to synchronize the user input with log output to prevent interrupting the user input.

Configuration Example

Synchronizing User Input with Log Output

Scenario	It is required to synchronize the user input with log output as follows: 1. Enable the synchronization function.
Configuration Steps	● Configure the synchronization function.
	FS# configure terminal FS(config)# line console 0 FS(config-line)# logging synchronous
Verification	● Run the **show running-config | begin line** command to display the configuration.
	FS#show running-config | begin line line con 0 logging synchronous login local As shown in the following output, when a user types in "vlan", the state of interface 0/1 changes and the related log is output. After log output is completed, the log module automatically displays the user input "vlan" so that the user can continue typing. FS(config)#vlan *Aug 20 10:05:19: %LINK-5-CHANGED: Interface GigabitEthernet 0/1, changed state to up *Aug 20 10:05:19: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/1, changed state to up FS(config)#vlan

8.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears logs in the memory buffer.	**clear logging**

Displaying

Description	Command
Displays log statistics and logs in the memory buffer based on the timestamp from oldest to latest.	**show logging**
Displays log statistics and logs in the memory buffer based on the timestamp from latest to oldest.	**show logging reverse**
Displays syslog configurations and statistics.	**show logging config**
Displays log statistics of each module in the system.	**show logging count**

9 Configuring LED

9.1 Overview

Light Emitting Diode (LED) is a solid luminous semiconductor. It serves as an indicator light to show AP's working status in different colors.

The following part only introduces LED.

Protocols and Standards

N/A

9.2 Application

N/A

9.3 Features

FSproducts support one or multiple LEDs to display AP's working status. For example, the LED on an Ethernet interface blink when there comes the data flow. It is controlled through GPIO or CPLD ports with different lighting, such as solid green, blinking green, blinking red and so on. By observing the LED, you can easily tell AP's working status and faults.

SuperLight LED includes basic function mode and expert diagnosis mode. Expert diagnosis function is enabled by default.

9.4 Configuration

Configuration Item	Configuration Suggestion & Relevant Command	
Configuring AP location.	(Optional) It is used to locate an AP. For rack APs, specify the slot ID for every RF card. For non-rack APs, the *slot-id* parameter is invalid.	
	led on	Turn on the LED to locate an AP.
Configuring Quiet Mode.	(Optional). It is used to enable LED quiet mode.	
	quiet-mode session	Enable LED quiet mode.

9.4.1 Configuring AP Location

Configuration Effect

- Turn on LEDs for AP location.

Notes

- Disable the configuration after location or the lighting of LEDs no longer changes.

Configuration Method

Configuring AP Location

- Optional configuration.
- Enable this configuration before AP location, and disable it after that.

Command	**led on**
Parameter Description	-
Defaults	This function is disabled by default.
Configuration Mode	AP configuration mode
Usage Guide	-

Check Method

- Check whether the location LED is on the AP.

Configuration Examples

Locating AP 00d0.f822.33bc

Scenario	N/A
Configuration Steps	Configure AP location on the AC.
AC	FS# configure terminal FS(config)# ap-config 00d0.f822.33bc FS(ap-config)# led on
Verification	Check whether the location LED is on the AP.

Common Mistakes

N/A

9.4.2 Configuring Quiet Mode

Configuration Effect

- All LEDs on an AP are off when this command takes effect.

Notes

- You must configure the effective time for the quiet mode at first.

Configuration Method

Configuring session

- Optional configuration.

- Create a session before the configuration of the quiet mode.
- Configure the effective time for the session.

Command	**schedule session** *sid* **time-range** *n* **period** *day1* [**to** *day2*] **time** *hh1:mm1* **to** *hh2:mm2*
Parameter Description	*sid*: scheduled session ID. *n*: scheduled session period No. *day1*: scheduled session period; day 1indicates the start date, in the range of { sun | mon | tue | wed | thu | fri | sat }. **to** *day2*: the end date, only one day of the interval by default. **time** *hh1:mm1* **to** *hh2:mm2*: scheduled session time. hh1:mm1 is the start time and hh2:mm2 the end time in the range from 0 to 23 hours and 0 to 59 minutes.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	Configure a session at first.

Configuring Quiet Mode

- Optional configuration.
- Configuring LED quiet mode.

Command	**quiet-mode session** *session-num*
Parameter Description	session-num: specifies the session ID.
Default Configuration	This function is disabled by default.
Configuration Mode	AP configuration mode
Usage Guide	Configure a session at first.

Check Method

- All LEDs are off when the system time is within the session interval.

Configuration Examples

Configuring LED Quiet Mode from Monday 11pm to Tuesday 7am Every Week

Configuration Steps	• Configure a session. • The following example configures the session ID for the quiet mode.

	FS# configure terminal FS(config)#schedule session 1 FS(config)#schedule session 1 time-range 1 period Mon time 23:00 to 7:00 FS(config)#ap-config 00d0.f822.33bc FS(config-ap)#quiet-mode session 1
Verification	When the system time is within the session interval, all LEDs on the AP are off.

Common Mistakes

- Configured session ID does not exist.

9.5 Monitoring

N/A

10 Configuring Exception Alarm

10.1 Overview

An exception alarm is an email that is sent to the device administrator when a device exception occurs. With the email, the administrator can learn about device running information and change configuration or perform other processing according to the exception, thereby ensuring proper running of different functions and the device.

An exception alarm may indicate a device attack, a high CPU temperature, a traffic limit excess problem or the like, which is implemented through cooperation of different modules. For example, the CPU temperature is monitored by the drive. When the CPU temperature reaches a threshold, relevant information will be sent to the exception alarm module. For another example, traffic is monitored by the flow control module. When the traffic amount reaches a threshold, relevant information will be sent to the exception alarm module as well.

Protocol Specifications

- RFC821: Simple Mail Transfer Protocol, SMTP

10.2 Applications

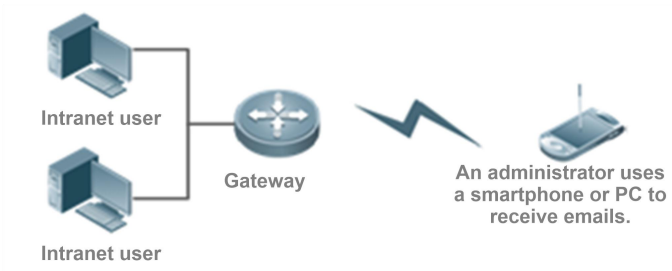
Application	Description
Applying Exception Alarm Upon Device Attack	A device generates an exception alarm upon an attack.

10.2.1 Applying Exception Alarm Upon Device Attack

Scenario

1. When a device is attacked from an intranet IP address, the anti-attack module collects information upon detecting the attack and notifies the exception alarm module of the attack.
2. The exception alarm module encapsulates the exception information into an email body and sends the information to a specified mailbox.
3. The administrator logs in to the Web portal of the gateway to process the intranet attack, for example, shields the attacker.

Figure 9-1



Deployment

- Configure a DNS server on the gateway and connect the gateway to the intranet.

10.3 Features

Basic Concepts

SMTP Server

The mailing procedure is as follows:

1. An email is sent to the SMTP server first.
2. The SMTP server classifies the email and sends the email to the SMTP server of the receiver.
3. The SMTP server of the receiver forwards the email to the mailbox of the receiver.

Figure 9- 2 shows the working principle.

Figure 9- 2

```
             +----------+                +----------+
+------+     |          |                |          |
| User |<-->|          |      SMTP      |          |
+------+     |  Sender- |Commands/Replies| Receiver-|
+------+     |   SMTP   |<-------------->|    SMTP  |     +------+
| File |<-->|          |    and Mail    |          |<-->| File |
|System|     |          |                |          |     |System|
+------+     +----------+                +----------+     +------+

              Sender-SMTP                Receiver-SMTP

                     Model for SMTP Use
```

SMTP working mode

The SMTP server refers to the Sender-SMTP in the preceding figure, which functions as a post office of the sender.

Common email client software such as Foxmail and Outlook plays the role of the User or File System in the preceding figure.

The mailing procedure of the exception alarm module is similar to that of the preceding software. Though the exception alarm module requires the sender to enter an email address and password, the mailing success rate is high.

Before using the exception alarm module, users must configure the SMTP server and email address and password.

Overview

Feature	Description
Exception Alarm	Monitors devices and functions and notifies the user of any exception that is detected.
Mail Service	Enables the mail service.
Receiving Mailbox	Configures a mailbox for receiving exception alarm information.
Mailing Frequency	The information timeliness is subject to the alarm mailing frequency. The smaller the frequency, the more timely the mailing. In other cases, a great number of emails may be received, for example, if an intranet attack occurs.

10.3.1 Exception Alarm

This function monitors devices and functions and notifies users of any exception that is detected.

Working Principle

- **Alarm Options**

There are many alarm options such as high CPU temperature, device attack, and traffic limit excess. The alarm options are monitored by multiple modules.

Users can configure alarm options, and the device will send any exception information about the options to a specified mailbox. Unselected options will be ignored even if any exception occurs.

Related Configuration

- **Enabling Exception Alarm Module**

This function is disabled by default.

Run the **feedback user enable** command to enable the exception alarm module.

- **Ignoring Alarm Options**

Supported alarm options are monitored by default. At present, supported alarm options include high CPU temperature, device attack, bandwidth limit excess, flow control exception, and high main board temperature.

Run the **feedback ignore** command to ignore an alarm option. The alarm option will be ignored even if any exception occurs.

10.3.2 Mail Service

A gateway constructs an email and sends the email to a specified mailbox.

Working Principle

- **Enabling Mail Service**

Enable the mail service.

- **SMTP Server**

A server that sends an email according to SMTP is referred as the Sender-SMTP. The SMTP server functions as a post office of the sender.

At present, many common mailboxes, for example, qq.com, 163.com, and Sina.com, support SMTP. Some mailboxes may require users to log in to the mailboxes to enable the SMTP service. The URL of an SMTP server can be queried from the mailbox web pages. For example, the URL of the QQ SMTP server is qq.smtp.com.

- **Email Address and Password**

The entered email address and password are used as sender information and encapsulated into an email. All email addresses that support SMTP are available.

Related Configuration

- **Enabling Mail service**

This function is enabled by default.

Run the **mail-service enable** command to enable the mail service.

Configuring SMTP Server

No SMTP server is configured by default.

The URL of an SMTP server can be queried from the mailbox website.

Run the **mail-client smtp server** command to configure an SMTP server.

Configuring Email Address and Password

No email address and password are configured by default.

At present, common mailboxes, for example, qq.com, 163.com, and Sina.com, are available.

The SMTP server is enabled for some mailboxes by default, and is disabled for others by default. If the mail service fails, log in to the mailbox using a browser to enable the SMTP service.

Run the **mail-client username** command to configure the email address and password.

10.3.3 Receiving Mailbox

A receiving mailbox is used to receive exception alarm emails. Generally, the mailbox of the network administrator is set as a receiving mailbox.

Working Principle

The receiving mailbox receives emails sent by a device. If multiple receiving mailboxes are configured, all these mailboxes will receive emails.

A receiving mailbox is equivalent to a receiver.

Related Configuration

Configuring Receiving Mailbox

No receiving mailbox is configured by default.

A maximum of six receiving mailboxes can be configured.

10.3.4 Mailing Frequency

After a device detects an exception, the alarm email transmission interval is subject to the mailing frequency.

Working Principle

Mailing Frequency

Emails are sent regularly. If the mailing frequency is set to one hour, the exception alarm module sends exception information that is detected within the past one hour.

Related Configuration

Configuring Mailing Frequency

The mailing frequency is one hour by default.

Run the **feedback frequency** command to configure the mailing frequency. The value ranges from 5 to 10,080 (unit: minute). A smaller value indicates a higher mailing frequency. To ensure timely receiving of alarm information, set the mailing frequency to a small value. To avoid receiving too many emails, set the mailing frequency to a great value.

10.4 Configuration

Configuration	Description and Command	
Configuring Basic Information of Exception Alarm Module	(Mandatory) It is used to configure basic information of the exception alarm module.	
	feedback user enable	Enables the exception alarm module.
	mail-service enable	Enables the mail service. The mail service is enabled by default.
	mail-client smtp server	Configures the SMTP server.
	mail-client username	Configures the email address and password.
	feedback subscriber	Configures the alarm receiving mailbox.
Configuring Mailing Frequency	(Optional) It is used to configure the mailing frequency.	
	feedback frequency	Configures the mailing frequency.
Configuring Source IP Address of Mail Service in Public Network Mode	It must be configured in public network mode. In other modes, it is not configured.	
	mail-service source	Configures the source IP address of the mail service. It must be configured in public network mode. In other modes, it is not configured.

10.4.1 Configuring Basic Information of Exception Alarm Module

Configuration Effect

- With the necessary functions of the exception alarm module, enable the device to encapsulate alarm information as an email body and send the email to a specified mailbox.
- Configure a maximum of six email addresses to receive emails.

Notes

- The URL of the SMTP server and the email address and password are used for mailing. Make sure that they are correctly configured.
- The email receiving address indicates a mailbox that receives the alarm information. Multiple email addresses can be configured. The email receiving address can be the same as the email address configured on the exception alarm module for mailing.

Configuration Steps

Enabling Feedback Module

- Mandatory. It is disabled by default.

Enabling Mail service

- Mandatory. It is enabled by default.

Configuring SMTP Server

- Mandatory.

Configuring Email Address and Password

- Mandatory.

Configuring Alarm Receiving Mailbox

- Mandatory. Set the email receiving address to the email address configured on the exception alarm module for mailing.
- Configure a maximum of six email addresses to receive emails.

Verification

Run the **mail-client check** command to check email configuration. If the configuration is correct, the email address configured on the exception alarm module for mailing will receive a test email.

Related Commands

Enabling Exception Alarm Module

Command	**feedback user enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling Mail Service

Command	**mail-service enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring SMTP Server

Command	**mail-client smtp server** *addr*
Parameter Description	**server** *addr*: Indicates the IP address of an SMTP server.

Command Mode	Global configuration mode
Usage Guide	The SMTP server can be queried from the mailbox page.

Configuring Receiving Mailbox

Command	**feedback subscriber** *mail-addr*
Parameter Description	**subscriber** *mail-addr*: Indicates the email receiving address.
Command Mode	Global configuration mode
Usage Guide	Multiple email addresses can be configured to receive emails. A maximum of six addresses can be configured.

Configuration Example

Enabling Exception Alarm Module and Configuring Basic Information

Configuration Steps	Enable the feedback module and mail service. Configure the IP address of the sender server and email address and password, and then configure the receiving email address.
	FS# configure terminal FS(config)# feedback user enable FS(config)# mail-service enable FS(config)# mail-client smtp server smtp.126.com FS(config)# mail-client username FS@126.com password ****** FS(config)# feedback subscriber UserA@FS.com.cn UserB@126.com UserC@qq.com FS(config)# end
Verification	Check whether relevant configuration is correct.
	FS# mail-client check
	Connect to smtp server. OK! Login to smtp server. OK! Send a test mail. OK! Check OK!

Common Errors

- The SMTP server is incorrect.

- The email address or password is incorrect.
- The SMTP service of the receiving mailbox is not enabled.

10.4.2 Configuring Mailing Frequency

Configuration Effect

- Change the email transmission frequency. A smaller value indicates more timely mailing.

Notes

- If the frequency value is too small, a great number of emails will be sent in a short period of time when the device is faulty.
- If the frequency value is too large, emails cannot be sent in a timely manner when the device is faulty.

Configuration Steps

- Set the mailing frequency to one hour by default. The mailing frequency can be not configured unless otherwise specified.
- In the event of a device fault, set the mailing frequency to a large value to avoid receiving a great number of emails within a short period of time.

Related Commands

Configuring Mailing Frequency

Command	**feedback frequency** *min*
Parameter Description	**frequency** *min*: Indicates a mailing frequency (unit: minute). The value ranges from 5 to 10,080.
Command Mode	Global configuration mode
Usage Guide	The mailing frequency is one hour by default.

Configuration Example

Configuring Mailing Frequency as One Hour

Configuration Steps	Configure the mailing frequency as one hour.
	FS# configure terminal FS(config)# feedback frequency· 60 FS(config)# end
Verification	N/A

10.4.3 Configuring Source IP Address of Mail Service in Public Network Mode

Configuration Effect

- Configure the source IP address in public network mode. Otherwise, alarm emails cannot be sent.

Notes

- The configuration is mandatory in public network mode. Otherwise, alarm emails cannot be sent. In other modes, the configuration must not be performed.

Configuration Steps

- No source IP address is configured by default. Configure the source IP address in public network mode.

Related Commands

Configuring Source IP Address

Command	**mail-service source** *ip*
Parameter Description	*ip*: Indicates a source IP address. The default value is the IP address configured on the LAN interface. The configuration is mandatory if the Internet can be accessed through an IP address on the LAN interface, but not an IP address on the WAN interface.
Command Mode	Global configuration mode
Usage Guide	It must be configured in public network mode. In other modes, it is not configured.

Configuration Example

Configuring Source IP Address as 1.1.1.1

Configuration Steps	Configure a source IP address as 1.1.1.1.
	FS# configure terminal FS(config)# mail-service source 1.1.1.1 FS(config)# end
Verification	N/A

10.5 Monitoring

Displaying

Description	Command
Displays currently supported alarm options.	**show feedback items**

Displays email configuration to check whether it is correct. Run this command after the IP address of the SMTP server and email address and password are configured.	**mail-client check**

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs the exception alarm switch.	**debug feedback info**

11 Configuring HTTP Service

11.1 Overview

Hypertext Transfer Protocol (HTTP) is used to transmit Web page information on the Internet. It is at the application layer of the TCP/IP protocol stack. The transport layer adopts connection-oriented Transmission Control Protocol (TCP).

Hypertext Transfer Protocol Secure (HTTPS) is an HTTP supporting the Secure Sockets Layer (SSL) protocol. HTTPS is mainly used to create a secure channel on an insecure network, ensure that information can hardly be intercepted, and provide certain reasonable protection against main-in-the-middle attacks. At present, HTTPS is widely used for secure and sensitive communication on the Internet, for example, electronic transactions.

Protocols and Standards

- RFC1945: Hypertext Transfer Protocol -- HTTP/1.0
- RFC2616: Hypertext Transfer Protocol -- HTTP/1.1
- RFC2818: Hypertext Transfer Protocol Over TLS -- HTTPS

11.2 Applications

Application	Description
HTTP Application Service	Users manage devices based on Web.
Remote HTTP Upgrade Service	The HTTP upgrade function is used to upgrade files.

11.2.1 HTTP Application Service

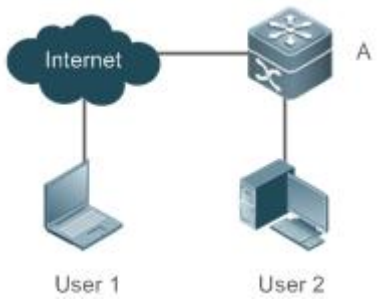
Scenario

After the HTTP service is enabled, users can access the Web management page after passing authentication by only entering **http://IP address of a device** in the browser of a PC. On the Web page, users you can monitor the device status, configure devices, upload and download files.

Take the following figure as an example to describe Web management.

- Users can remotely access devices on the Internet or configure and manage devices on the Local Area Network (LAN) by logging in to the Web server.
- According to actual conditions, users can choose to enable the HTTPS or HTTP service or enable the HTTPS and HTTP services at the same time.
- Users can also access the HTTP service of devices by setting and using HTTP/1.0 or HTTP/1.1 in the browser.

Figure 10- 1



Remarks	A is a FSdevice. User 1 accesses the device through the Internet. User 2 accesses the device through a LAN.

Deployment

- When a device runs HTTP, users can access the device by entering **http://IP** address of the device in the browser of a PC.
- When a device runs HTTPS, users can access the device by entering https://IP address of the device in the browser of a PC.

11.2.2 Remote HTTP Upgrade Service

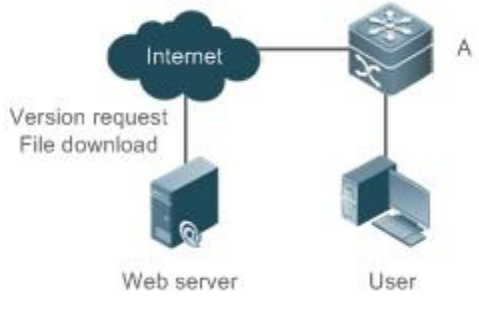
Scenario

HTTP remote upgrade means that a device is connected to a remote HTTP server as a client and realizes local file upgrade by obtaining files from the server. The default domain name of a Web server provided by FSis **FSOS.FS.com.cn**.

Take the following figure as an example. Use the HTTP remote upgrade function to upgrade files.

- A device obtains upgrade files from a FSserver every day on a scheduled basis.
- Download the latest files from the server and update the upgrade device.

Figure 10- 2



Remarks	A is a FSdevice. User is a PC user. Web server is a FSserver.

Deployment

- When a device runs HTTP, directly send a command to the device through the browser and obtain the latest upgrade files from the Web server.

11.3 Features

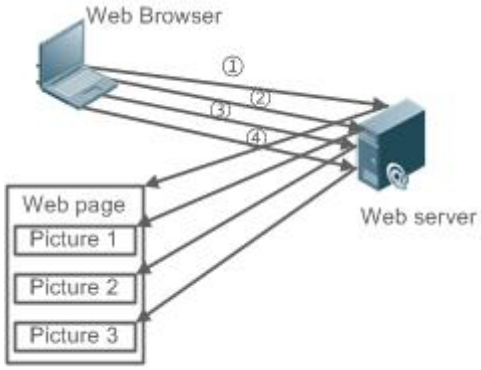
Basic Concepts

↘ HTTP Service

The HTTP service refers to transmission of Web page information on the Internet by using HTTP. HTTP/1.0 is currently an HTTP version that is the most widely used. As one Web server may receive thousands or even millions of access requests, HTTP/1.0 adopts the short connection mode to facilitate connection management. One TCP connection is established for each request. After a request is completed, the TCP connection is released. The server does not need to record or trace previous requests. Although HTTP/1.0 simplifies connection management, HTTP/1.0 introduces performance defects.

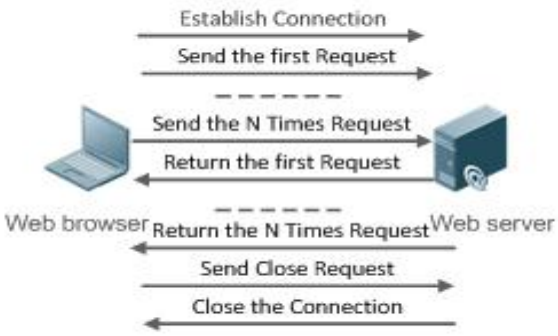
For example, a web page my need lots of pictures. However, the web page contains not real picture contents but URL connection addresses of the pictures. In this case, the browser sends multiple requests during access. Each request requires establishing an independent connection and each connection is completely isolated. Establishing and releasing connections is a relatively troublesome process, which severely affects the performance of the client and server, as shown in the following figure:

Figure 10- 3



HTTP/1.1 overcomes the defect. It supports persistent connection, that is, one connection can be used to transmit multiple requests and response messages. In this way, a client can send a second request without waiting for completion of the previous request. This reduces network delay and improves performance. See the following figure:

Figure 10- 4



At present, FSdevices support both HTTP/1.0 and HTTP/1.1.

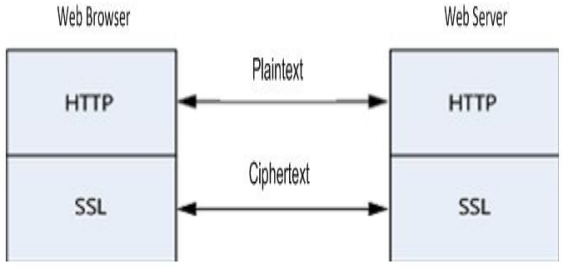
Which HTTP version will be used by a device is decided by the Web browser.

HTTPS Service

The HTTPS service adds the SSL based on the HTTP service. Its security basis is the SSL. To run HTTPS properly, a server must have a Public Key Infrastructure (PKI) certificate while a client may not necessarily need one. The SSL protocol provides the following services:

- Authenticating users and servers and ensuring that data is sent to the correct client and server.
- Encrypting data to prevent data from being stolen midway.
- Maintaining data integrity and ensuring that data is not changed during transmission.

Figure 11- 5



HTTP Upgrade Service

HTTP upgrade includes local HTTP upgrade and remote HTTP upgrade.

- During a local upgrade, a device serves as an HTTP server. Users can log in to the device through a Web browser and upload upgrade files to the device to realize file upgrade on the device.

- During a remote upgrade, a device is connected to a remote HTTP server as a client and realizes local file upgrade by obtaining files from the server.

Features

Feature	Description
HTTP Service	Users log in to devices through Web pages to configure and manage devices.
Remote HTTP Upgrade Service	A device is connected to a remote HTTP server as a client and realizes local file upgrade by obtaining files from the server.
Local HTTP Upgrade Service	Upgrade files are uploaded to a device to realize file upgrade on the device.

11.3.1 HTTP Service

HTTP is a service provided for Web management. Users log in to devices through Web pages to configure and manage devices.

Working Principle

Web management covers Web clients and Web servers. Similarly, the HTTP service also adopts the client/server mode. The HTTP client is embedded in the Web browser of the Web management client. It can send HTTP packets and receive HTTP response packets. The Web server (namely HTTP server) is embedded in devices. The information exchange between the client and the server is as follows:

- A TCP connection is established between the client and the server. The default port ID of the HTTP service is 80 and the default port ID of the HTTPS service is 443.
- The client sends a request message to the server.
- The server resolves the request message sent by the client. The request content includes obtaining a Web page, executing a CLI command, and uploading a file.
- After executing the request content, the server sends a response message to the client.

Related Configuration

Enabling the HTTP Service

By default, the HTTP service is disabled.

The **enable service web-server** command can be used to enable HTTP service functions, including the HTTP service and HTTPS service.

The HTTP service must be enabled so that users can log in to devices through Web pages to configure and manage devices.

Configuring an HTTP Service Port

By default, the HTTP service port ID is 80.

The **http port** command can be used to configure an HTTP service port ID. The value range of the port ID is 80 and 1025 to 65535.

By configuring an HTTP service port ID, you can reduce the number of attacks initiated by illegal users on the HTTP service.

Configuring an HTTPS Service Port

By default, the HTTPS service port ID is 443.

The **http secure-port** command can be used to configure an HTTPS service port ID. The value range of the port ID is 443 and 1025 to 65535.

By configuring an HTTPS service port ID, you can reduce the number of attacks initiated by illegal users on the HTTPS service.

11.3.2 Remote HTTP Upgrade Service

A device is connected to a remote HTTP server as a client and realizes local file upgrade by obtaining files from the server.

Working Principle

- The server is connected. When the server is connected, the server address configured by the user is connected in preference. If the server address cannot be connected, the server addresses in the local upgrade files are connected in turn.
- The versions of service modules of the local device are sent to the server.
- The server resolves the versions and provides a file download list.
- Based on the file download list, the device is connected to the file server and downloads upgrade files. Different downloaded files can be used to connect different servers.
- The device upgrades files.

Related Configuration

Configuring an Upgrade Server Address

By default, the server address is the official website of FS, namely **FSOS.FS.com.cn**.

The **http update server** command can be used to configure the address and port ID of a remote HTTP upgrade server. If you specify the server, you need to contact FSR&D personnel to help create an upgrade server and obtain the latest version of service modules in real time. You are advised not to configure an upgrade server but use the default FSofficial website for upgrade. The upgrade server on FSofficial website is maintained by dedicated R&D personnel.

During an HTTP upgrade, the server address configured by using the command is connected in preference. If the server address cannot be connected, server addresses recorded locally are connected in turn. If none of the server addresses can be connected, the upgrade cannot be performed.

Configuring an HTTP Upgrade Mode

By default, HTTP uses the automatic upgrade mode.

The **http update mode** command can be used to set the HTTP upgrade mode to manual upgrade.

Configuring the HTTP Automatic Upgrade Time

By default, the remote automatic HTTP upgrade time is random.

The **http update time** command can be used to change the automatic upgrade time. Only a time point in each day can be configured and the precision reaches minute.

After this command is run, if the upgrade mode is automatic upgrade, the device detects and upgrades files on the server at the configured time every day.

Configuring Upgrade through the Management Port

By default, an HTTP upgrade is performed through a common port. Certain devices support the management port. The **http update set oob** command can be used to perform an upgrade on devices through the management port.

Detecting Upgrade Files on the HTTP Server

By default, the function of detecting HTTP upgrade files is disabled.

The **http check-version** command can be used to detect upgrade files on the HTTP server.

This command can be run to detect the latest files on the server.

Manually Upgrading Files

Run the **http update** command to manually upgrade files.

11.3.3 Local HTTP Upgrade Service

When a device serves as the HTTP server, users can log in to the device through a Web browser and upload upgrade files (including component package and Web package) to the device or directly upload files to the device through Trivial File Transfer Protocol (TFTP).

Working Principle

- A component package or Web package is uploaded through the local upgrade function provided by Web.
- After successfully receiving a file, the device checks the version for its validity.
- After the file check is successful, if the file is a Web package, perform the upgrade directly; if the file is a component package, decide whether to perform the upgrade in the browser by restarting the device.

Related Configuration

Updating a Subsystem Component

By default, a device does not upgrade subsystem components uploaded through a browser or TFTP.

To upgrade a subsystem component, you must restart the device.

11.4 Configuration

Configuration	Description and Command	
Configuring the HTTP Service	(Mandatory) It is used to enable the HTTP service.	
	enable service web-server	Enables the HTTP service.
	http port	Configures an HTTP service port.
	http secure-port	Configures an HTTPS service port.
Configuring a Remote HTTP Upgrade	(Mandatory) It is used to realize a remote HTTP upgrade.	
	http update server	Configures an HTTP upgrade server.
	http update mode	Configures an HTTP upgrade mode.
	http update time	Configures the HTTP automatic upgrade time.

Configuration	Description and Command	
	http update set oob	Configures upgrade through the management port.
	http check-version	Detects upgrade files on an HTTP server.
	http update	Manually upgrades files.

11.4.1 Configuring the HTTP Service

Configuration Effect

After the HTTP service is enabled on a device, users can log in to the Web management page after passing authentication and monitor the device status, configure devices, upload and download files.

Configuration Steps

Enabling the HTTP Service

- Mandatory
- If there is no special requirement, enable the HTTP service on FSdevices. Otherwise, the Web service is inaccessible.

Configuring an HTTP Service Port

- If an HTTP service port needs to be changed, the HTTP service port must be configured.
- If there is no special requirement, the default HTTP service port 80 can be used for access.

Configuring an HTTPS Service Port

- If an HTTPS service port needs to be changed, the HTTPS service port must be configured.
- If there is no special requirement, the default HTTPS service port 443 can be used for access.

Verification

- Enter http://IP address of the device: service port to check whether the browser skips to the authentication page.
- Enter https://IP address of the device: service port to check whether the browser skips to the authentication page.

Related Commands

Enabling the HTTP Service

Command	**enable service web-server** [**http** | **https** | **all**]
Parameter Description	**http** | **https** | **all**: Enables the corresponding service. **http** indicates enabling the HTTP service, **https** indicates enabling the HTTPS service, and **all** indicates enabling the HTTP and HTTPS services at the same time. By default, the HTTP and HTTPS services are enabled at the same time.
Command Mode	Global configuration mode.
Usage Guide	If no key word or **all** is put at the end of the command when the command is run, the HTTP and HTTPS services are enabled at the same time. If the key word **http** is put at the end of the command, only the HTTP service is enabled; if the

	key word **https** is put at the end of the command, only the HTTPS service is enabled. The **no enable service web-server** or **default enable service web-server** command is used to disable the corresponding HTTP service. If no key word is put at the end of the **no enable service web-server** or **default enable service web-server** command, the HTTP and HTTPS services are disabled.

Configuring an HTTP Service Port

Command	**http port** *port-number*
Parameter Description	*port-number*: Configures an HTTP service port. The value range is 80 and 1025 to 65535.
Command Mode	Global configuration mode.
Usage Guide	Run the command to set an HTTP service port.

Configuring an HTTPS Service Port

Command	**http secure-port** *port-number*
Parameter Description	*port-number*: Configures an HTTPS service port. The value range is 443 and 1025 to 65535.
Command Mode	Global configuration mode.
Usage Guide	Run the command to set an HTTPS service port.

Configuration Example

Managing one FSDevice by Using Web and Logging in to the Device through a Web Browser to Configure Related Functions

- Log in to the device by using the admin account configured by default.
- To improve security, the Web browser is required to support both HTTP and HTTPS for access.
- The user is required to configure an HTTP service port to reduce the number of attacks initiated by illegal users on HTTP.

Scenario **Figure 10-6**	
Configuration Steps	● Enable the HTTP and HTTPS services at the same time. ● Set the HTTP service port ID to 8080 and the HTTPS service port ID to 4430.
A	A#configure terminal A(config)# enable service web-server A(config)# http port 8080 A(config)# http secure-port 4430
Verification	Check HTTP configurations.

A	A# show web-server status http server status: enabled http server port: 8080 https server status:enabled https server port: 4430

Common Errors

- If the HTTP service port is not the default port 80 or 443, you must enter a specific configured service port in the browser. Otherwise, you cannot access devices on the Web client.

11.4.2 Configuring a Remote HTTP Upgrade

Configuration Effect

A device is connected to a remote HTTP server as a client and realizes local file upgrade by obtaining files from the server.

Notes

- Before configuring the domain name of an HTTP upgrade server, enable the Domain Name System (DNS) on the device and configure the DNS address. Otherwise, the device cannot communicate with FSofficial website.

Configuration Steps

Configuring the HTTP Upgrade Server

- To change the server address and port ID for an HTTP remote upgrade, you must configure the HTTP upgrade server and contact FSR&D personnel for help.
- If there is not special requirement, the upgrade server does not need to be configured and the default address can be used. The device communicates with FSofficial website and automatically obtains the latest versions of service modules. The upgrade server on FSofficial website is maintained by dedicated personnel.

Configuring an HTTP Upgrade Mode

- If you require the HTTP manual upgrade mode, you must configure it.
- If there is no special requirement, the HTTP upgrade mode is automatic upgrade by default.

Configuring the HTTP Automatic Upgrade Time

- To change the HTTP automatic upgrade time, you must configure the upgrade time.
- If there is not special requirement, the upgrade time does not need to be configured. The device automatically detects versions at random time. If you need to configure the upgrade time, you are advised to set the upgrade time to a time point early in the morning to avoid occupation of device traffic in rush hours.

Configuring Upgrade through the Management Port

- If an upgrade needs to be performed through the management port, you must configure the upgrade.

- By default, an upgrade is performed through a common port by default. If an upgrade is performed through the management port, run the command to configure the upgrade. Otherwise, the upgrade fails.

Detecting Upgrade Files on the HTTP Server

- If upgrade files on the HTTP server need to be detected, you must perform the configuration.
- If there is not special requirement, the configuration does not need to be performed because an upgrade is performed automatically.

Manually Upgrading Files

- Mandatory
- If there is no special requirement, configure a manual upgrade file on each device.

Verification

- Run the ping command to verify that the device can be connected to the server.
- Run the http check-version command to obtain versions of related files on the device.

Related Commands

Configuring the HTTP Upgrade Server

Command	**http update server** { *host-name* | *ip-address* } [**port** *port-number*]
Parameter Description	*host-name*: Domain name of the server. *ip-address*: Server address. **port** *port-number*: Server port ID. The value range is 1 to 65535 and the default value is 80.
Command Mode	Global configuration mode.
Usage Guide	Run this command to configure the server address and port ID for HTTP upgrade. During an HTTP upgrade, connect the server address configured by running this command. If the server address cannot be connected, connect server addresses recorded locally in turn. If none of the servers can be connected, the upgrade cannot be performed. The system records the address or addresses of one or more upgrade servers. These addresses cannot be modified. The server address may not be configured because the local upgrade file records addresses of possible upgrade servers. By default, the DNS needs to be enabled on a device and the DNS address needs to be configured.

Configuring an HTTP Upgrade Mode

Command	**http update mode manual**
Parameter Description	**manual**: Manual upgrade mode.
Configuration	Global configuration mode.

mode	
Usage Guide	Run the command to configure an HTTP upgrade mode. Run the command to set the HTTP upgrade mode to manual mode. After the **no http update mode manual** command is run, the HTTP upgrade mode is set to automatic mode. When it is time for automatic upgrade, the system detects upgrade files on the server and automatically downloads and upgrades the files.

Configuring the HTTP Automatic Upgrade Time

Command	**http update time daily** *hh:mm*
Parameter Description	*hh:mm*: Specific upgrade time in the format of hour:minute (24-hour system).
Configuration mode	Global configuration mode.
Usage Guide	Run this command to configure the automatic HTTP upgrade time. Devices are connected to the Web server (FSOS.FS.com.cn) at the fixed time every day to detect possible upgrade files. You can view obtained files on the Web page. After the **no http update time daily** command is run, the device upgrade time is random.

Configuring Upgrade through the Management Port

Command	**http update set oob**
Parameter Description	N/A
Configuration mode	Global configuration mode.
Usage Guide	Run this command to perform an HTTP upgrade through the management port. If you run the **no http update set oob** command, an HTTP upgrade is performed through a common port. This command can be run on only the devices that support the management port.

Detecting Upgrade Files on the HTTP Server

Command	**http check-version**
Parameter Description	N/A
Configuration mode	Privileged mode
Usage Guide	Run this command to detect types of upgrade files. The latest upgrade files are detected.

Manually Upgrading Files

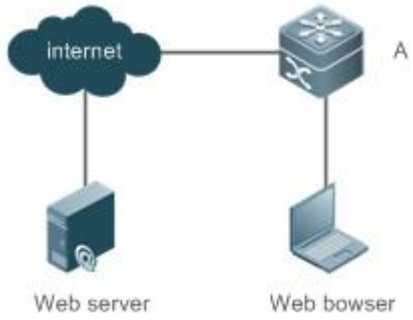
Command	**http update** { **all** | *string* }

Parameter Description	**all**: Upgrades all service modules. *string*: Name of the service module to be upgraded.
Configuration mode	Privileged mode
Usage Guide	Run this command to manually to upgrade the specified service module or all service modules.

Configuration Example

Using the HTTP Remote Upgrade Function to Upgrade Files

- A device obtains upgrade files on FSserver and downloads the upgrades the files at 02:00 every day.
- Check the current upgrade files.
- Download the latest files from the server provided by FSand update the upgrade device.

Scenario **Figure 10-7**	
Configuration Steps	● Configure the DNS. ● Set the scheduled remote monitoring time to 02:00 on the device. ● Obtain upgrade files from the remote server. ● Download files from the server and update the device.
A	A#configure terminal A(config)# ip domain-lookup A(config)# ip name-server 192.168.58.110 A(config)# http update time daily 02:00 A(config)# http check-version A(config)# end A# http update all
Verification	N/A

Common Errors

- When the DNS is disabled, a connection cannot be established between a device and a server.

11.5 Monitoring

Displaying

Description	Command
Displays the configuration and status of the Web service.	**show web-service**

12 Configuring PATCH-UPGRADE

12.1 Overview

PATCH-UPGRADE manages automatic upgrade, manual upgrade, and manual uninstallation of devices' patch packages.

12.2 Applications

Application	Description
PATCH-UPGRADE Application Scenarios	Describe basic scenarios and functions of PATCH-UPGRADE.

12.2.1 Typical Application Scenarios

Scenario

PATCH-UPGRADE applies to the following scenarios:

- Patch upgrade: When a new hot patch is released, PATCH-UPGRADE downloads the patch package from the MACC server and automatically installs it to upgrade the patch. PATCH-UPGRADE also allows manual deletion or upgrade of patch packages.

Deployment

Automatic patch upgrade is enabled for devices by default without special configuration.

12.3 Features

Basic Concepts

Patch Package

A patch package contains patch files used to fix some bugs. After an upgrade, some components will be updated to fix bugs.

Patch Package Status

A patch package has four states: no patch, installed, loaded, and permanently loaded. In loaded and permanently loaded states, a patch package replaces components to be updated and takes effect.

Loading Period

The loading period indicates the time range when a device automatically loads a patch package after the device installs the patch package.

Overview

Feature	Description
PATCH-UPGRADE	Upgrade, roll back, or uninstall a patch based on configuration.

12.3.1 PATCH-UPGRADE

PATCH-UPGRADE downloads the latest patch package based on server configuration, performs a patch upgrade or rollback based on device configuration, and allows manual upgrade and uninstallation upon exceptions.

Working Principle

PATCH-UPGRADE communicates with the MACC server to obtain the latest patch information on the server. If the patch version on the server is later than that on the device, PATCH-UPGRADE automatically downloads the patch. In automatic patch upgrade mode, the patch is automatically installed on the device after being downloaded. However, the patch is loaded only in the loading period. A patch is permanently loaded after it is successfully loaded for more than five days. If the device restarts within five days, the patch returns to the installed state and the manual patch upgrade mode is enabled. In manual patch upgrade mode, no automatic update is performed. You need to manually enter the upgrade or uninstallation command to upgrade or uninstall the patch package.

Related Configuration

Configuring Patch Upgrade

The automatic patch upgrade mode is enabled by default.

Run the **patch-upgrade** command to configure the patch upgrade mode, modify the automatic loading period, and enable manual patch upgrade or uninstallation.

Displaying Patch Upgrade

Run the **show patch-upgrade** command to display the patch status, configuration, upgrade logs, and other information.

12.4 Configuration

Configuration	Description and Command	
Configuring Patch Upgrade	Mandatory.	
	patch-upgrade	Configures patch upgrade.

12.4.1 Configuring Patch Upgrade

Configuration Effect

- Configure the patch upgrade mode.
- Modify the automatic loading period.
- Configure manual patch upgrade or uninstallation.

Configuration Steps

Configuring the Patch Upgrade Mode

- Optional. The automatic patch upgrade mode is enabled by default. If an automatic upgrade fails, the manual patch upgrade mode is used.

Configuring the Automatic Loading Period

- Optional. The automatic loading period is 03:00 to 04:00 every day by default.

Configuring Manual Upgrade or Uninstallation

- Optional. For manual patch upgrade or uninstallation for a device, the device must have a patch package installed.

Verification

- Display patch upgrade configuration.

Related Commands

Configuring the Patch Upgrade Mode

Command	**patch-upgrade set-mode** {**auto** | **manual** }
Parameter Description	
Command Mode	Privileged EXEC mode
Usage Guide	This command sets the patch upgrade mode to automatic or manual.

Configuring the Automatic Loading Period

Command	**patch-upgrade set-active-time start** *hh:mm* **end** *hh:mm*
Parameter Description	*hh:mm*: Indicates the hour and minute.
Command Mode	Privileged EXEC mode
Usage Guide	This command sets the automatic patch loading period.

Configuring Manual Upgrade

Command	**patch-upgrade manual-active**
Parameter Description	
Command Mode	Privileged EXEC mode
Usage Guide	This command enables manual upgrade when a device has a patch package installed.

Configuring Manual Uninstallation

Command	**patch-upgrade delete**
Parameter Description	

Command Mode	Privileged EXEC mode
Usage Guide	This command enables manual uninstallation when a device has a patch package installed.

Displaying Configuration and Status of PATCH-UPGRADE

Command	**show patch-upgrade state**
Parameter Description	
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to display the status and configuration of PATCH-UPGRADE.

Displaying Logs of PATCH-UPGRADE

Command	**show patch-upgrade log**
Parameter Description	
Command Mode	Privileged EXEC mode
Usage Guide	This command displays logs of PATCH-UPGRADE.

12.5 Monitoring

Displaying

Description	Command
Displays configuration and status of PATCH-UPGRADE.	**show patch-upgrade state**
Displays logs of PATCH-UPGRADE.	**show patch-upgrade log**

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs the PATCH-UPGRADE tracking switch.	**debug patch-upgrade info**
Debugs the PATCH-UPGRADE error information tracking switch.	**debug patch-upgrade error**
Debugs the PATCH-UPGRADE HTTP	**debug patch-upgrade http-info**

download tracking switch.	

13 Configuring WEB-UPGRADE

Overview

WEB-UPGRADE is a web package management and upgrade module of the FSOS system and is responsible for upgrade and query of devices' web components. After WEB-UPGRADE upgrades web components of a device, clients can install a version that is more stable or contains more features.

Protocols and Standards

- N/A

13.1 Applications

Application	Description
Web Package Upgrade	Upgrade devices' web components and display web package information.

13.1.1 Web Package Upgrade

Scenario

After a web component package is upgraded, original web files on the device are updated and web functions are enhanced.

Compared with the upgrade of a system component package, the upgrade of a web component package takes a shorter time and the device does not need to be restarted after the upgrade.

Deployment

Before a web package upgrade for a device, place the web package in the root directory of the TFTP server, download the package to the device through the network, and run the local upgrade command to complete the upgrade. Alternatively, copy the web package to a USB flash drive or SD card, insert the USB flash drive or SD card to the device, and run the upgrade command to complete the upgrade.

13.2 Features

Basic Concepts

N/A

Overview

Feature	Description
Web Package Upgrade	Upgrade the web package locally.

13.2.1 Web Package Upgrade

Working Principle

A web package upgrade is to replace web files in a device with files in the web package.

After the upgrade is completed, the original web package will not be automatically deleted and needs to be manually deleted.

Related Configuration

Upgrading the Web Package

Store the upgrade file in the local file system of a device and run the **web-upgrade** command to complete the upgrade.

13.3 Configuration

Configuration	Description and Command	
Upgrading the Web Package Locally	Basic function. It is used to upgrade the web package.	
	web-upgrade *url*	Upgrades the web package stored in the local path (indicated by *url*) of the device.

13.3.1 Upgrading the Web Package Locally

Configuration Effect

- Upgrade the web package.

Configuration Steps

Upgrading the Web Package

- Before an upgrade, download the web package to a local directory of a device.
- Run the web-upgrade command to perform an upgrade.
- Manually delete the downloaded web package.

Verification

Run the **show web-upgrade** command to display and check web package information.

Related Commands

Upgrading the Web Package Locally

Command	**web-upgrade** *url*
Parameter Description	*url*: Indicates the web package storage path in the file system of a device.
Command Mode	Privileged EXEC mode

Usage Guide	N/A

Displaying Web Package Information

Command	**show web-upgrade**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	N/A

Configuration Example

Upgrading the Web Package Locally

Scenario	Before an upgrade, copy the web package to a local directory of the device using either of the following methods:
	● Use a file system command, such as **copy** to copy the web package to the file system of the device. Then, run the **web-upgrade** *url* command to upgrade the web package in the local file system.
	● Copy the web package to a USB flash drive or SD card and insert the USB flash drive or SD card to the device. Run the **web-upgrade** *url* command to upgrade the installation package in the USB flash drive or SD card.
	After the upgrade is completed, the original web package will not be automatically deleted. To delete the package, run the **delete** command.
Configuration Steps	● Run the **copy tftp** command to download the web package to the local **tmp** directory of the device.
	FS#copy tftp://172.21.3.137/web.gz tmp:web.gz Press Ctrl+C to quit !!!!!!!!!!!!!!!! Copy success.
	● Run the local upgrade command to upgrade the web package.
	FS# web-upgrade tmp:web.gz Upgrade web package start... MD5 a310c329b917fdc992864f8287d83681 Web version[2018.6.8.07->2018.6.8.10] Upgrade info [OK] Upgrade web package succeeded.
	● Run the **delete** command to delete the original web package in the local **tmp** directory.

	FS#delete tmp:web.gz
	FS#
Verification	● Run the **show web-upgrade** command to display information about the web package used by the device. If the information is updated, the upgrade is successful.
	FS# show web-upgrade Version : 2018.6.8.10 Md5 : a310c329b917fdc992864f8287d83681 Size : 9012807 Build : 2018-06-08 10:37:41 Compatible : EG* Incompatible : EG2100-P|EG680-P

Chapter 4 Behavior Management

1. Configuring Layer2/3 Classification
2. Configuring APP-IDENTIFY
3. Configuring App Route
4. Configuring App Proxy
5. Configuring User Session Limit
6. Configuring Flow Control
7. Configuring Flow Audit
8. Configuring Content Audit
9. Configuring Line Quality

1 Configuring Layer 2/3 Classification

1.1 Overview

To control the action of the internal network subscribers, a device needs first to identify their data flow. Layer 2/3 classification can detect and identify the data flow based on VLAN tag, source IP address and destination IP address of packets, and then classify the data flow into different objects. The device takes corresponding action on various objects to control the action of the internal network subscribers.

Objects of layer 2 and layer 3 include VLANs, subscribers, networks, authenticated subscribers, and built-in authentication, where:

VLAN: a configured object based on the VLAN ID of the internal network subscriber. It allows data flow classification based on the VLAN tag of the packet. In gateway mode, VLAN is invalid. In bridge mode, the default match of all data flow will be the corresponding VLAN of the Native VLAN in the bridge. If the Native VLAN does not have any corresponding VLAN, then data flow will match with the default VLAN "any".

Subscriber: a configured object based on the IP address and MAC address of the internal subscriber. It allows data flow classification based on the source IP address and source MAC address of the packet. When it fails to match with the configured subscriber, the data flow will match with the system default subscriber "any". MAC address matching will be preferential when both MAC address and IP address are matched.

Network: a configured object based on the internal network address visited by both internal and external network subscribers. It allows data flow classification based on the destination IP address of the packet. When it fails to match with the configured network, the data flow will match with the system default network "any".

Auth-sub: an automatically generated policy based on the accounts and IP address synchronized by an external server. It allows data flow classification based on the source IP address of the packet. When no external server is synchronized to the device, then the data flow will match with the system default auth-sub "any".

Built-in authentication: Web authentication performed by using the database and portal server built in the device. There are two types of local databases: subs database and local database. This module only involves the subs database. Layer 2/3 classification is applicable to small and medium-sized companies, supporting action control and audit of different departments according to their VLANs and IP address segments.

One VLAN ID can only belong to one VLAN; one IP address can only belong to one subscriber and network.

1.2 Application

Application	Description
Restricting Access to External Networks in Offices	In some of the offices, all staff except leaders are forbidden to access external networks.
Exempting Specific Users from Audit and Flow Control	In the university scenario, content audit and flow control are performed on network access of all students.
Preferentially Guaranteeing Access to External Servers	The rate of download from and that of upload to the server in the headquarters need to be guaranteed.
Implementing Built-in Perception-free Authentication	Middle- and small-sized enterprises apply local authentication and subsequently require perception-free go-online.
Filtering MAC Binding	Only clients with the MAC address and IP address manually bound are allowed to access the network.

1.2.1 Restricting Access to External Networks in Offices

Scenario

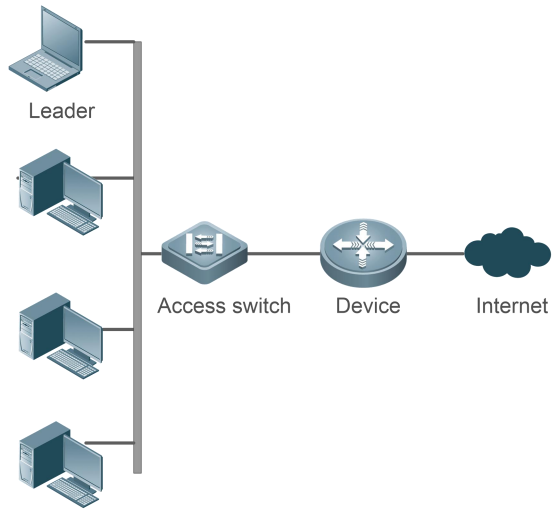
All data flows for accessing external networks are forbidden, except data flows of leaders. Once identified, the data flows of leaders will be specially processed and allowed according to the objects to which they belong.

For example, as shown in Figure 1–1, access from intranet users to the Internet is restricted in small-sized office networks.

Intranet users can communicate with each other but cannot access the Internet.

Leaders can access the Internet.

Figure 1-1



Remarks	A layer-2 network environment is required inside the device and NAT is not allowed. Otherwise, data flows cannot be identified.

Deployment

Enable layer 2/3 classification commands on the device.

Enable global shielding mode on layer 2/3 of the device.

Configure User Object A that is based on the IP address or MAC address of the leader's client.

Set the whitelist attribute of User Object A.

1.2.2 Exempting Specific Users from Audit and Flow Control

Scenario

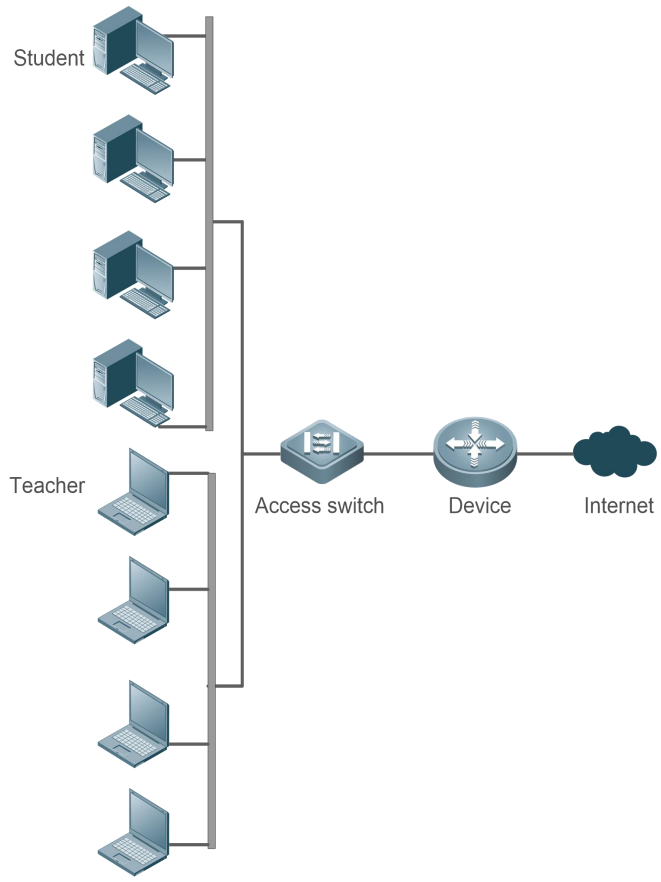
Data flows respectively from network segments for students and teachers are identified and then processed differently.

For example, as shown in Figure 1–2, in the university scenario, flow control and audit need to be performed on online behaviors of the students, but online behaviors of the teachers do not need to be audited.

Content audit and flow control are performed on identified data flows of the students.

Content audit and flow control are not performed on identified data flows of the teachers.

Figure 1-2



Remarks	A layer-2 network environment is required inside the device and NAT is not allowed. Otherwise, data flows cannot be identified.

Deployment

Enable layer 2/3 classification, content audit, and flow control on the device.

Configure a global content audit and flow control policy on the device for all users.

Configure User Object A that is based on the network segment for the teachers.

Set the monitoring-free attribute for User Object A.

1.2.3 Preferentially Guaranteeing Access to External Servers

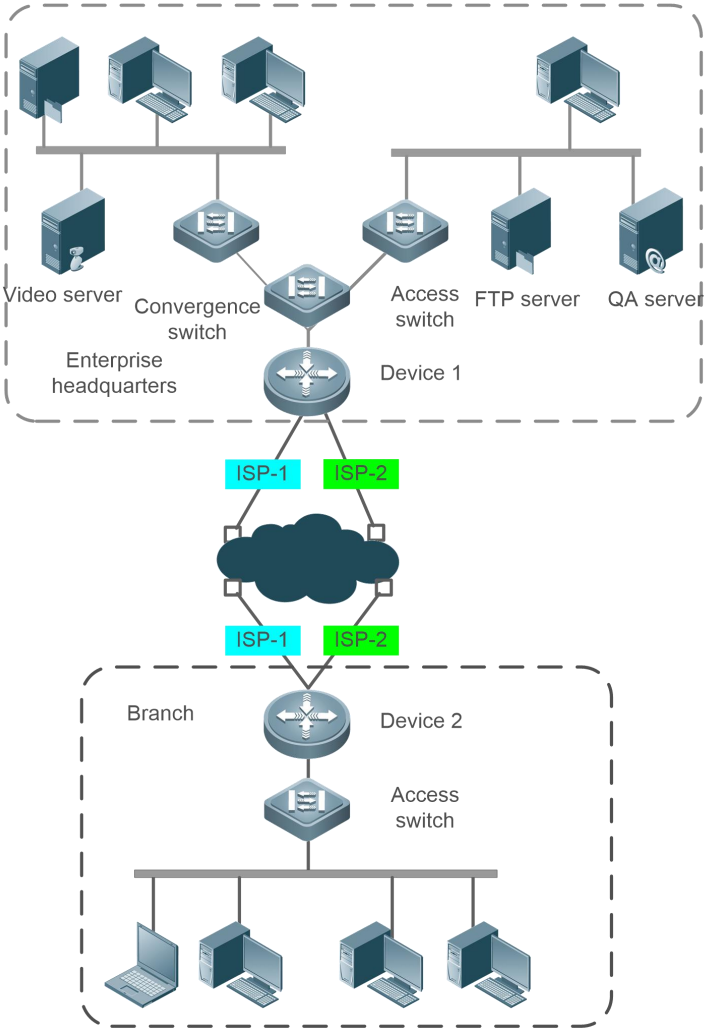
Scenario

For example, as shown in the following Figure 1–3, in the headquarters-branch scenario, data flows from branches for accessing the headquarters servers need to be preferentially guaranteed.

Flow control is performed on access from branches to external networks and the rate of flows is limited.

The rate of download from the headquarter server to a branch and that of upload from a branch to the headquarters server are preferentially guaranteed.

Figure 1-3



Remarks	A layer-2 network environment is required inside the device and NAT is not allowed. Otherwise, data flows cannot be identified.

Deployment

Enable layer 2/3 classification and flow control on the device.

Configure a global flow control policy on the device for all users.

Enable Device 2 to dial up to Device 1 through a VPN.

On Device 2, configure Network Object A that is based on the IP address of the internal server of the headquarters.

Configure a flow control policy based on Network Object A and adjust the priority of the policy to the highest.

1.2.4 Synchronizing Real-Name Accounts

Scenario

Real-name accounts registered with external servers can be synchronized, including the SAM+, SMP, and ESS servers.

Deployment

Enable layer 2/3 classification commands on the device.

Enable the server association function and configure the SAM+ association or SNMP association.

1.2.5 Filtering MAC Binding

Scenario

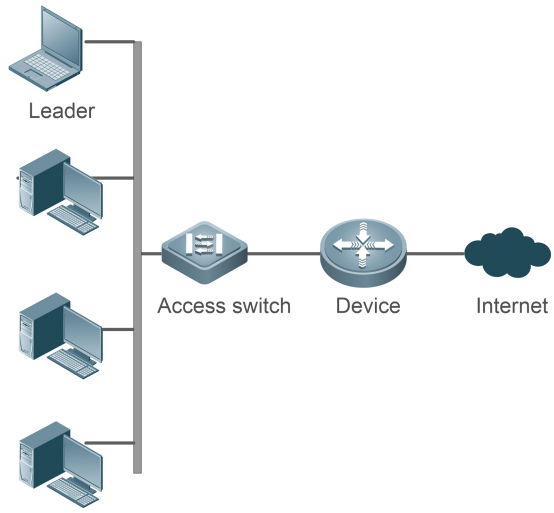
The administrator expects that all associated clients have their IP addresses and MAC addresses manually bound, to forbid access to the Internet from invalid clients.

For example, as shown in Figure 1–4, invalid clients are forbidden to access the Internet.

In strict verification mode, a client with the MAC address and IP address bound can access the Internet normally.

Clients without the MAC address and IP address bound are not allowed to access the Internet.

Figure 1–4



Remarks	N/A

Deployment

Enable the strict verification mode on the device.

Manually configure static ARP entries for valid clients on the device.

1.3 Features

Basic Concepts

VLAN, Subscriber, Network and Auth-subs

VLAN is a configured object based on the VLAN ID of the internal network subscriber.

Subscriber is a configured object based on the IP address and MAC address of the internal subscriber.

Network is a configured object based on the internal network address visited by both internal network subscribers.

Auth-sub is an automatically generated policy based on the accounts and IP address synchronized by an external server.

Object and Object-group

As VLAN does not have layered structure, it composes no group.

Network includes single IP network, range network and network-group who does not have configured IP address.

Subscriber includes configured subscribers with password, IP address or MAC address and subscriber group with none of them.

The IP node of an authenticated subscriber corresponds with its exclusive real-name account and information of its account group. It is automatically generated.

Conflict Objects

The existence of the configured name, IP address or MAC address or the configured path inconsistent with the layered structure in actual group constitutes the conflict between the configured object and the existing one.

Account, Single-way-bind and Two-way-bind

A subscriber set with password can be used as an authentication account. Then the configured IP address and MAC address are bound with the account, which can be configured with single-way-bind or two-way-bind.
By single-way-bind, the account can only be bound with the IP address or MAC address that may be used by other accounts.
By two-way-bind, the account can only be bound with the IP address or MAC address, which is solely used by the account. Accounts not bound with the IP address or MAC address are not limited by the used IP address or MAC address.

Object Index

An object index only identifies one exclusive object node. It is calculated according to the memory address of the configured object in the kernel, which is consistent with the object index in user space. The identified data flow will record corresponding indexes of different objects. And the following traffic control or audit module will query about the object information of the data flow managed by the subscriber.

Data Flow Classification

Data flow will be classified into different objects according to the VLAN tag, source IP address and MAC address in the packet as well as their configured information.

Built-in Perception-free Authentication

Data of the user static object is used for authentication and verification and an MAC address will be recorded after the initial authentication succeeds. When the user accesses the Internet subsequently, no username or password is required and the MAC address is directly verified, thereby implementing perception-free authentication.

Strict Verification Mode

In this mode, only a client that has its IP address and MAC address bound and that can be correctly identified can access the Internet.

Overview

Feature	Description
Data Flow Classification	Identifies data flow of different subscribers to control their action.

1.3.1 Data Flow Classification

Data flows will be classified into different objects according to their configured information like IP address and MAC address. By controlling the policies of different objects, you can control differentiated actions on diversified data flows to which various objects belong.

Working Principle

Data flow classification consists of object management and object identification.

Object Management

Administrator will configure subscribers according to the IP address and MAC address of the subscriber and associate and store the name, IP address and index of the subscriber in memory.

Object Identification

Layer 2/3 classification will query and match the configured object data according to the VLAN tag, IP address and MAC address in the packet and classify various data flows into different objects. The pointer of the classified data flow will be recorded in the private flow space and the index of the object will be recorded in packet. With the index recorded in data flow, the following traffic control or audit module will query about corresponding information managed by the subscriber and then through controlling the policies of different objects, the diversified data flow control over different objects will be achieved.

Related Configuration

Enabling Layer 2/3 Classification Feature

Layer 2/3 classification is enabled by default.
Use the layer23 classify enable command to enable Layer 2/3 classification.
Use the no form of the layer23 classify enable command to disable the function.

Configuring Subscriber, Network and Auth-subs

System configures subscriber groups for Defalut_Group and VPN_Group and network-group for Out-Sever by default.
Use the command subscriber staticnamenamestrparent parstr [[[ip-host ip-addr] [mac mac-addr] | ip-subnet subnetmask | ip-range start end] [password pwd_str{ two-way-bind | single-way-bind}] | [passwordpwd_str] to configure subscribers.
Use the no subscriber staticnamenamestr command to eliminate subscribers.
Use the command network-groupnamenamestr[parent parent] [ip-host ip-addr|ip-subnet subnet mask| ip-range start end]] to configure networks.
Use the nonetwork-groupnamenamestr to eliminate networks.
Use the vlan-groupnamevlanvid-list to configure VLANs.
Use the novlan-groupname command to eliminate VLANs.

Configuring Strict Verification Mode

The strict verification mode is disabled by default.
Run the layer23 strict-verification enable command to enable the strict verification mode.
Run the no layer23 strict-verification enable command to disable the strict verification mode.

1.3.2 Built-in Perception-free Authentication

The subs static object is used to conduct the initial verification on the username and password during Web authentication. The MAC address is recorded after the verification succeeds. No username or password is required for subsequent access authentication and access is allowed provided that the MAC address verification succeeds.

Working Principle

The initial access authentication uses the username and password for verification, and the subsequent access uses the MAC address for verification.

Verification Process

A user enters the username and password for Web authentication. The AAA server selects the user object based on the subs

authentication method and verifies the username and password. An MAC address will be recorded after the subs authentication succeeds. When the user subsequently accesses the Internet, for IPoE, the MAC address is obtained for verification by the AAA server based on the subs database. An authentication success message will be returned after the MAC verification succeeds, and then the user can access the Internet.

Related Configuration

Configuring Perception-free Mode to the subs Directory

The perception-free mode of the subs database is disabled by default.

Run the layer23 subs-mab enable command to enable the perception-free mode of the subs database.

Run the no layer23 subs-mab enable command to disable the perception-free mode of the subs database.

1.4 Configuration

Configuration	Description and Command	
Configuring Layer 2/3 Classification Feature	(Mandatory) It is used to identify the subscriber of the data flow, otherwise, the audit and traffic control over subscriber will be invalid.	
	layer23 classify enable	Enables Layer 2/3 Classification Feature.
Configuring Layer 2/3 Global Deny-mode	(Optional) Unless the subscriber has whitelist attributes, all packets will be dropped by default.	
	layer23 deny-mode enable	Enables layer 2/3 deny-mode in global configuration mode.
Configuring Strict Verification Mode	(Optional) After this function is enabled, the incorrect IP-MAC binding will be discarded.	
	layer23 strict-verification enable	Enables strict verification mode.
Configuring Perception-free Mode of Subs Database	(Optional) Enables Web authentication first.	
	layer23 subs-mab enable	Enable the perception-free mode of the subs database.
Configuring Layer 2/3 Off-line State Detect by Flow	(Optional) By enabling this function, the device will be forced to go off-line for not reaching the flow threshold within the specified period.	
	layer23 flow-detect enable	Enables layer 2/3 flow detect.
	layer23 flow-detect flow 0	Configures getting off-line without flow.
	layer23 flow-detect time-interval 15	Configures getting off-line without flow in 15 minutes.
Configuring Network Objects	Optional.	
	network-group *str1* **move to parent** *str2*	Moves the network-group.
	network-group export { **txt** | **csv** } *filename*	Exports configuration of the current network into an external file.

	network-group import { **txt** | **csv** } *filename* [**overwrite**]	Imports a network into the current configuration.
	network-group name *namestr* [**parent** *parent*] [**ip-host** *ip-addr* | **ip-subnet** *subnet mask* | **ip-range** *start end*]]	Configures networks.
	network-group rename *oldname newname*	Renames the network.
Configuring Subscriber	Optional.	
	subscriber *str1* **move to parent** *str2*	Moves the subscriber.
	subscriber allow *string* **privilege** { **none** | { [**webauth**] [**vpn**] [**login**] } }	Sets account privilege of the subscriber.
	subscriber export { **txt** | **csv** } *filename*	Imports the subscriber file into configuration.
	subscriber import { **txt** | **csv** } *filename* [**overwrite**]	Exports configuration of the subscriber into an external file.
	subscriber rename *oldname newname*	Renames the subscriber.
	subscriber set *namestr* **attribute** { **avoid-monitor** [**flow-monitor**] | **deny** | **release** | **vip** | **auth-deny** | **pwd-edit** |	Sets the attributes of the subscriber.
	subscriber static name *namestr* **parent** *parstr* [[[**ip-host** *ip-addr*] [**mac** *mac-addr*] | **ip-subnet** *subnet mask* | **ip-range** *start end*] [**password** *pwd_str* { **two-way-bind** / **single-way-bind** }] | [**password** *pwd_str*]]	Configures the subscriber.
Configuring VLAN Objects	Optional.	
	vlan-group *name* **vlan** *vid-list*	Configures VLAN objects.

1.4.1 Configuring Layer 2/3 Classification Feature

Configuration Effect

Classify data flows into different objects.

Make action control policies corresponding with different objects.

Notes

By disabling Layer 2/3 Classification, policies of audit and traffic control will be invalid.

By offloading kernel module, objects can still be configured and managed, but cannot be identified.

Configuration Steps

Enabling Layer 2/3 Classification

Mandatory.

If there is no special requirement, the function must not be disabled on the device, otherwise subscriber-based audit and traffic control cannot be proceeded.

Verification

Configure an object based on a IP address and use this IP address to pass through the device to visit external network.
Check whether this data flow in private flow space is identified as a correct object.
Check whether the object information displaying that the object is associated with proper number of flows.

Related Commands

Enabling Layer 2/3 Classification

Command	**layer23 classify enable**
Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	Layer 2/3 Classification supports object recognition based on VID, source IP address, or source MAC address or destination IP address.

Configuration Examples

Enabling Layer 2/3 Classification Feature on the Device

Configuration Steps	Enabling Layer 2/3 Classification on the device.
	FS# configure terminal FS(config)# layer23 classify enable FS(config)# end
Verification	Use the **show run** command to display whether there is the **layer23 classify enable** command in configuration file.

Common Errors

Policies based on subscriber are invalid and the switch of Layer 2/3 Classification is disabled.

1.4.2 Configuring Global Deny-mode

Configuration Effect

Forbid the internal network subscribers to visit external network.
Allow a minority of the subscribers on whitelist to visit external network.

Notes

The Layer 2/3 Classification feature must be enabled.

Configuration Steps

Optional.

Enabling Layer 2/3 Classification on the device and enabling layer 2/3 global deny-mode.

Verification

Use the show run command to display whether there is the layer23 deny-mode enable command in configuration.

Related Commands

Layer 2/3 Global Deny-mode

Command	**layer23 deny-mode enable**
Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	Running layer 2/3 deny-mode to drop all packets by default, except the subscriber is not denied (i.e. the subscriber is on the whitelist).

Configuration Examples

Enabling Layer 2/3 Deny-mode in Global Configuration Mode, While Allowing Subscriber A to Visit External Network

Configuration Steps	Enable deny-mode in global configuration on the device while configure whitelist attribute for Subscriber A.
	FS#configure terminal FS(config)# layer23 deny-mode enable FS(config)# subscriber static name A parent / ip-host 192.168.1.2 FS(config)#subscriber set A attribute release FS(config)# end
Verification	Visit external network using different IP addresses. ● Cannot visit external network with any IP address except 192.168.1.2. ● Can visit external network using IP address 192.168.1.2.

Common Errors

All subscribers cannot visit external network for improper configuration of layer 2/3 global deny-mode.

1.4.3 Configuring Strict Verification Mode

Configuration Effect

In this mode, limit a user with the IP address and MAC address unbound or incorrectly bound and forbid the user to access the Internet.

Notes

Before enabling this mode, bind the IP address and MAC address of a user.

The static ARP entry is the source of IP+MAC binding.

Configuration Steps

- Optional.

Enable this mode and bind the IP address and MAC address of a valid client.

Verification

Run the show layer23 strict-verification command to check whether the strict verification mode switch is enabled.

Related Commands

Strict Verification Mode

Command	**layer23 strict-verification enable**
Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	In this mode, packets from a client with the static ARP entry unbound or incorrectly bound will be directly discarded.

Configuration Example

Enabling the Strict Verification Mode and Allowing Only the test Account (1.1.1.1, 00d0.f822.33ef) to Access the Internet

Configuration Steps	Enable the strict verification mode and bind the IP address and MAC address of the test account.
	FS#configure terminal FS(config)# layer23 strict-verification enableFS(config)# end
Verification	Only the test account can be used to access the Internet: ● The test account can be used to access the Internet. ● The test account cannot be used to access the Internet once the IP address of the test account is changed ● Other clients cannot access the Internet via the IP address 1.1.1.1.

Common Errors

An IP/MAC/user conflict occurs.

1.4.4 Configuring Built-in Perception-free Mode

Configuration Effect

After the initial Web authentication succeeds, no authentication is required for subsequent access to the Internet.

Notes

The built-in perception-free mode needs to be used together with the Web authentication function.

Configuration Steps

- Optional.

Enable the subs perception-free mode after the Web authentication function is enabled.

Verification

Run the show run command to check whether the configuration information contains the layer23 subs-mab enable command.

Related Commands

subs Perception-free Mode

Command	**layer23 subs-mab enable**
Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	In subs perception-free mode, the MAC address will be recorded after the initial Web authentication succeeds, and no username or password but only the MAC address is directly verified for subsequent access.

Configuration Example

Enabling subs Perception-free Mode So That Web Authentication Is Omitted for User Object A After Initial Authentication

Configuration Steps	Enable the built-in Web authentication function on the device, configure the related username and password, and configure the subs perception-free mode.
	FS#configure terminal FS(config)# layer23 subs-mab enable FS(config)# end
Verification	After the initial Web authentication succeeds, enable the user to go offline and then go online again. ● The username and password are required for the initial Web authentication. ● The user can access the Internet directly without requiring the username or password after the user goes offline and then goes online.

1.4.5 Configuring Layer 2/3 Off-line State Detect by Flow

Configuration Effect

Force authenticated IP address without flow within a specific time interval to get off the line.

Notes

Getting off-line by flow detect is valid only for accounts authenticated and synchronized into layer 2/3.
Flow audit function should be enabled at the same time.

Configuration Steps

Optional.
Configuring web authentication after flow audit function and Layer 2/3 Classification are enabled on the device and configuring flow detect feature after the subscriber passed the authentication.

Verification

Use the show run command to display whether there is the layer23 flow-detect enable command and the corresponding flow and time parameters.
Configure flow-detect off-line after the device got online by web authentication, then observe whether it is forced to get off-line for not reaching the threshold of flow parameter in a specific time interval.

Related Commands

Layer 2/3 flow-detect Switch

Command	**layer23 flow-detect enable**
Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	By enabling layer 2/3 flow-detect, the online node will be forced to get off the line for not reaching the specified flow in specific time interval.

Configuring Layer 2/3 flow-detect Parameter

Command	**layer23 flow-detectflow** *flowrate*
Parameter Description	*flowrate*: flow parameter, unit: bit/s
Command Mode	Global configuration mode
Usage Guide	It is recommended to set flow parameter to the average value of the total flow in 30 seconds.

Configuring Time Interval Parameter for Layer 2/3 flow-detect

Command	**layer23 flow-detecttime-interval** *time*

Parameter Description	*time:* time parameter
Command Mode	Global configuration mode
Usage Guide	The online node will be forced to get off the line for not reaching the specified flow in specific time interval.

Configuration Examples

Enabling Layer 2/3 flow-detect and Configuring go-offline Without Traffic in 15 Minutes

Configuration Steps	Enabling global deny-mode on the device and configuring flow-detect off-line parameter at layer 2/3.
	FS#configure terminal FS(config)# layer23 flow-detect enable FS(config)# layer23 flow-detect flow 0 FS(config)#layer23 flow-detect time-interval FS(config)# end
Verification	Enable web authentication and getting off-line by layer 2/3 flow-detect. ● With IP address 192.168.1.2, use Account 1 to get online by authentication. ● Change PC IP address into 192.168.1.3 and use Account 2 to get online by authentication. ● IP address 192.168.1.2 without flow, wait for 15 minutes and observe that IP address 192.168.1.2 was forced to get off the line.

Common Errors

Misunderstand the flow parameter whose unit is bit/s but not the accumulated total flow.

Flow-detected off-line function requires flow audit.

1.4.6 Configuring Supporting One SAM+ Account Relating to Different Operators Feature

Configuration Effect

When One SAM+ account belongs to various operator groups, the information will be forwarded to the device and displayed.

Notes

This feature is configured only for the account synchronized by the SAM+ server.

Configuration Steps

- Optional.

By enabling link-SAM+ association, configuring this command to support issuing information of one SAM+ account belonging to various groups.

Verification

Use the show run command to display whether there is the layer23 sam-accip-relate enable command in configuration.

After enabling this feature, run the show auth-subs briefs command to display whether the name of the SAM+ account is composed with group name.

```
root(auth-subs group)
    smp_root(auth-subs group)
    sam_root(auth-subs group)
        CMII(auth-subs group)
            CMII:111:111(auth-subs group)
        CMCC(auth-subs group)
            CMCC:111:111(auth-subs group)
    webauth_root(auth-subs group)
```

Related Commands

One SAM+ Account Relating with Various Groups Switch

Command	**layer23 sam-accip-relate enable**
Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	By enabling the function, layer 2/3 will identify the real-name information synchronized from SAM+ server, including IP address, account and group. Because the device name is exclusive and belong to only one parent group, it is recommended to make up account name in **Group:Name:Account** form at the device to assure the nomenclature is exclusive. This function is available only for subscribers synchronized by SAM+ server.

Configuration Examples

Enabling SAM+ Account Relating with Various Groups

Configuration Steps	Enabling SAM+ account relating with various groups feature after enabling SAM+ account association.
	FS# configure terminal FS(config)# layer23 sam-accip-relate enable FS(config)# end
Verification	Enable SAM+ account association and SAM+ account belonging to various groups feature. ● Use the **show layer23 sam-acc** account to display the feature state. ● By the authenticated online of SAM+ server account, observe whether the account information synchronized by the SAM+ sever contains group name. ● Observe whether the configuration policy of SAM+ account group is valid.

Common Errors

The feature is only valid when SAM+ account association is enabled at the same time.

Non-SAM+ server accounts are not in favor.

1.4.7 Configuring Real-name Information Supported SCC Setting Feature

Configuration Effect

Make the real-name information in SCC configuration available for the release of authenticated IP addresses.

Notes

Normally, authentication of subscribers in batches is not enabled for consideration of the device performance, except the secondary authentication.

Configuration Steps

- Optional in CLI.

Validating this feature only after link-SAM+ association or SNMP association is enabled as well as real-name information is accepted.

Verification

Use the show run command to display whether there is the layer23 scc-attention enable command in configuration.
After enabling this feature, use the show layer23 state command to display its state.

Related Commands

Enabling SCC Real-name Information Setting Switch

Command	**layer23 scc-attention enable**
Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	After enabling the function, layer 2/3 will identify the real-name information synchronized from the server and set them in SCC module. It is commended not to enable this feature in general scenario for performance optimization. In a secondary authentication scenario, both access switch and the device are enabled to proceed authentication. After authenticated by access switch, no more secondary authentication is required and this feature should be enabled.

Configuration Examples

Enabling SCC Real-name Information Setting

Configuration Steps	Enabling SAM+ account relating with various groups feature after enabling SAM+ account association.
	FS#configure terminal FS(config)#layer23 scc-attention enable FS(config)# end

Verification	Enable SCC real-name information setting. ● Use the **show layer23 state** command to display the feature state. ● Use the **show run** command to display **layer23 scc-attention enable** command. ● Disable this function and use the **debug scc user author** command to display whether SCC entries contain authenticated IP addresses synchronized and managed by the subscriber.

Common Errors

This function is often applied together with real-name account information association on SAM+/SMP/ESS servers.

1.4.8 Configuring Network Objects

Configuration Effect

Correlate IP address with network name.

Perform special action control over different networks objects.

Notes

Layer 2/3 Classification must be enabled for the validation of the policy based on network objects.

The network names must differ from each other and one IP address can only match with one network-group.

Configuration Steps

Moving a Network Object

Optional.

Move a network object on the device to change the path of it.

Exporting the Network Object

Optional.

Export configuration of the current network object into an external file on the device.

Importing the Network Object

Optional.

Import the network information into the current configuration on the device.

Configuring the Network Object

Optional.

Configure the network object to correlate its name with IP address.

Renaming the Network Object

Optional.

Rename the network object without change its attributes and layered structure.

Verification

Configure a network object relating to one IP address and use an internal PC to visit the IP address configured by the network object.

Check whether the show run command contains the information configured by the network object.

Check whether the flow correctly matched with the network object in the layer 2/3 private flow space.

Related Commands

Moving a Network Object

Command	**network-group** *str1* **move to parent** *str2*
Parameter Description	*str1*-: name of the network object to be moved. *str2*-: name of the parent-network after moved.
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to change the path of a child-network on condition that the movement does not change other attributes of it and layered structures of its children.

Exporting the Network Object

Command	**network-group export** { **txt** | **csv** } *filename*
Parameter Description	*filename*-file name
Command Mode	Privileged EXEC mode
Usage Guide	This command is mainly to export in batches the configuration of the current system network into an external file.

Importing Network Objects

Command	**network-group import** { **txt** | **csv** } *filename* [**overwrite**]
Parameter Description	*filename*-file name
Command Mode	Privileged EXEC mode
Usage Guide	This command is mainly to import networks in batches into the current configuration. The syntax to write networks in the txt format file will be: each column for a network, and its element order will be: path, network name and IP address. Each element of a network should be separated with ",", and items without content can be blank but keep with ",", for example, the last column do not exist, then keep "," in the end of this column. The following is an example of a network record in ".txt" format: / All users/ User group 1, User 1,192.168.197.1 You can get "csv" format network file after editing in Microsoft Excel and saving it as ".csv". The syntax for the record

	in the file shall be: one record with 4 columns, including parent-network path, child-network name and child-network IP address.

Configuring the Network Object

Command	**network-group name** *namestr* [**parent** *parent*] [**ip-host** *ip-addr* | **ip-subnet** *subnet mask* | **ip-range** *start end*]]
Parameter Description	*namestr* - the network-group name *parent*- - the path of the parent-network *ip-addr* - single IP address *subnet* -start address of the IP address segment *mask* - mask *start* - start address of the IP address range *end* - end address of the IP address range
Command Mode	Global configuration mode
Usage Guide	Networks only have IP address information, which consists of IP address networks, IP address segment networks and IP address range networks. There is a default network "/", and when Layer 2/3 Classification is enabled and the destination IP of a packet does not match with any network, then the packet itself will match with the default network. If parent filed is not set, then the parent-network will be under the root by default.

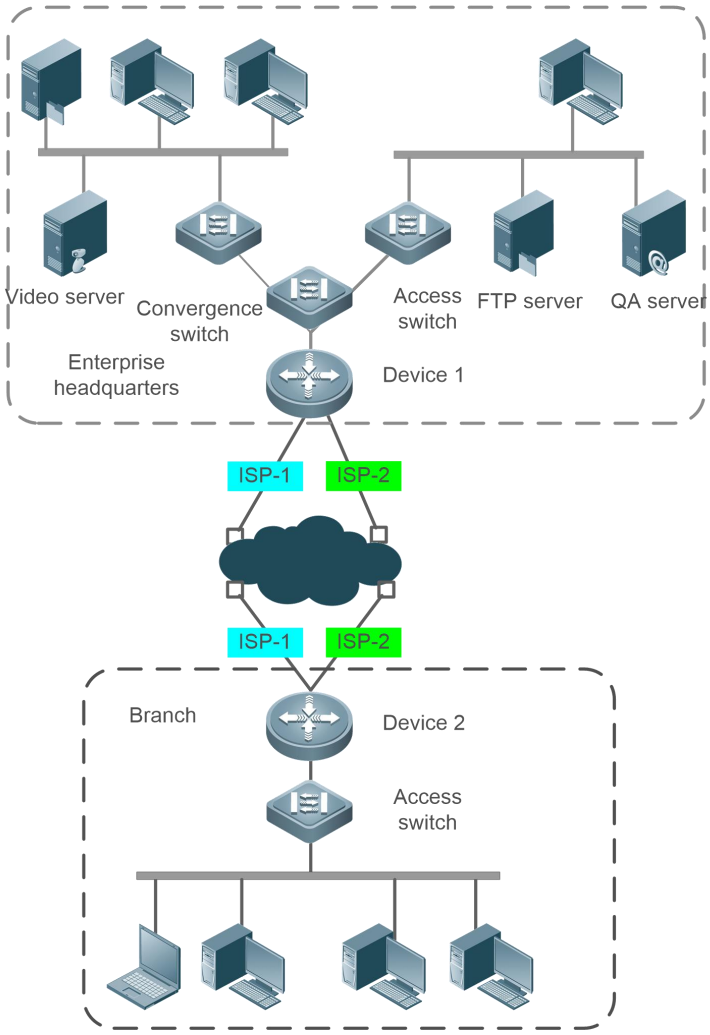
Renaming the Network Object

Command	**network-group rename** *oldname newname*
Parameter Description	*oldname* - name of the original network *newname* - name of the new network
Command Mode	Privileged EXEC mode
Usage Guide	This command is mainly to change the name of a network which will not change other attributes of the original network.

Configuration Examples

The following only introduces commands related with Layer 2/3 Classification.

Ensuring first to visit external servers and the IP address of internal server is 123.123.123.123.

Scenario **Figure 1–5**	
Configuration Steps	Enabling Layer 2/3 Classification. Device 2 dials up to Device 1 through a VPN. Configure Network Object A based on the IP address of the internal server in the headquarters. Configuring traffic control assurance policy based on Network A.
EG2	FS# configure terminal FS(config)# layer23 classify enable FS(config)# network-group name A parent / ip-host 123.123.123.123 FS(config)# end
Verification	Use the **show network-group by-name** *A* **kernel** command to display whether there is associated flow number. name flow dir index ip A 5 0 37160 123.123.123.123

Common Errors

Failure to enable Layer 2/3 Classification results in failed identification after the network object is configured.

The network-group was configured wrongly on basis of internal IP address, resulting in failure of matching.

1.4.9 Configuring Subscriber

Configuration Effect

Correlate IP address and MAC address with subscriber name.

Perform special action control over different subscribers.

Notes

Layer 2/3 Classification must be enabled for the validation of the subscriber-based policy.

The subscriber names must differ from each other and a two-way-bind IP address or MAC address can only belong to one subscriber.

Configuration Steps

- **Moving Subscriber**

Optional.

It used to move a subscriber on the device to change the parent of it.

- **Exporting Subscriber**

Optional.

It used to export configuration of the current subscriber into an external file on the device.

- **Importing Subscriber.**

Optional.

It used to import the subscriber information in the file into the current configuration on the device.

- **Configuring Subscriber**

Optional.

It used to configure the subscriber on the device to correlate its name with information like IP address, MAC address and password.

- **Renaming Subscriber**

Optional.

It used to rename the subscriber without change its attributes and layered structure.

- **Configuring Subscriber Privilege**

Optional.

It used to configure usage privilege of the subscriber account set with a password on the device as well as configure whether WEB and VPN authentication are valid for it.

- **Setting Special Attributes for the Subscriber**

Optional.

It used to configure special identifiers for the subscriber on gateway for specific treatment.

Verification

Configure two-way-bind for a subscriber and set deny attribute to it, then use this IP address to visit external network through the gateway.

Check whether the show run command contains the information configured by the subscriber.

Check whether the flow is correctly matched with the subscriber in the layer 2/3 private flow space.

Fail to use this IP address to visit external networks while succeed in visiting external networks by using other IP addresses.

Related Commands

Moving a Subscriber

Command	**subscriber** *str1* **move to parent** *str2*
Parameter Description	*str1*-: name of the subscriber to be moved. *str2*-: name of the parent-sub after moved.
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to change the path of a subscriber, which will not change other attributes of it and the layered structures of its children.

Exporting the Subscriber

Command	**subscriber export** { **txt** | **csv** } *filename*
Parameter Description	*filename*-file name
Command Mode	Privileged EXEC mode
Usage Guide	This command is mainly to export in batches the configuration of the current system subscribers into an external file.

Importing the Subscriber

Command	**subscriber import** { **txt** | **csv** } *filename* [**overwrite**]
Parameter Description	*filename*-file name
Command Mode	Privileged EXEC mode
Usage Guide	This command is mainly to import subscribers in batches into the current configuration. The syntax to write subscribers in the txt format file will be: each column for a subscriber, and its element order will be: path, account name, password, IP address, MAC address and flag of two-way bind. Each element of a subscriber should be separated by ",", and items without content can be blank but with "," left; for example, the last column does not exist, then leave "," in the end of this column. The following is an example of a subscriber record in ".txt" format: / All users/ User group 1, User 1, 192.168.197.1

	You can get "csv" format network file after editing in Microsoft Excel and saving it as ".csv". The syntax for the record in the file shall be: one record with 4 columns, including parent-sub path, subscriber name password, IP address, MAC address and flag of two-way bind.

Configuring the Subscriber

Command	**subscriber static name** *namestr* **parent** *parstr* [[[**ip-host** *ip-addr*] [**mac** *mac-addr*] | **ip-subnet** *subnet mask* | **ip-range** *start end*] [**password [0 | 6 | 7]** *pwd_str* { **two-way-bind** / **single-way-bind** }] | [**password [0 | 6 | 7]** *pwd_str*]] [**phone** *phone_number*]
Parameter Description	*namestr* - the network-group name *parstr*- the path of the parent-network *ip-addr* - single IP address *mac-addr* - MAC address *subnet* -start address of the IP segment *mask* - mask *start* - start address of the IP range *end* **-** end address of the IP range *pwd_str* **-** password *phone_number*-phone number
Command Mode	Global configuration mode
Usage Guide	The IP address of the subscribers must not collide with that of any subscriber except the parent-subs, and MAC address must not collide with any subscriber. By IP address, subscribers consist of single IP address subscriber, IP address segment subscriber and IP address range subscriber; by MAC address, subscriber with MAC address and subscriber without MAC address, where single IP address subscribers may at the same time have MAC address and IP address segment, while IP address range subscribers can only have MAC address or IP address segment. MAC address matching will be prior when both MAC address and IP address are matching. There is a default network " / ", and when Layer 2/3 Classification is enabled and the source IP address of a packet does not match with any subscriber, then the packet itself will match with the default network. A normal subscriber set with password can be used as an account. Single/two-way-bind is available only for accounts with IP address or MAC address, and by two-way-bind, the account is bound with IP address or MAC address. In this way, the account can only use a segment of IP address or MAC address, which is solely used by the account. By single-way-bind, the account can only use the bound IP address or MAC address that may be used by other accounts. Accounts without bind with IP address or MAC address are not limited by the address of using IP address or MAC address, while accounts with IP address and MAC address is two-way bound by default. With internal authentication, IP address will be automatically added to the account, while IP addresses will be added to webauth_root when their online accounts are out of the range of the tree. After you configure a mobile number, the SMS authentication is supported.

Renaming the Subscriber

Command	**subscriber rename** *oldname newname*
Parameter Description	*oldname* - name of the original subscriber *newname* - new name of the subscriber
Command Mode	Privileged EXEC mode
Usage Guide	This command is mainly to change the name of a subscriber which will not change other attributes of the original.

Configuring the Subscriber Privilege

Command	**subscriber allow** *string* **privilege** { **none** | { [**webauth**] [**vpn**] [**login**] } }
Parameter Description	*string* - name of the subscriber
Command Mode	Global configuration mode
Usage Guide	You can set the privilege of the account to allowing none, one, or two or all of login, VPN and WEB authentication.

Setting Special Attributes for the Subscriber

Command	**subscriber set** *namestr* **attribute** { **avoid-monitor**[**flow-monitor**] | **deny** | **release** | **vip** | **auth-deny** | **pwd-edi**}
Parameter Description	*namestr* - name of the subscriber
Command Mode	Global configuration mode
Usage Guide	Using monitoring attributes will not enable flow control, content audit and application identification about the subscriber, but you can set flow-monitor to control the flow used by the subscriber. Deny attributes are invalid in deny mode, and the packet of the subscriber shall be dropped when deny attributes are set in normal mode. Deny attributes are in effective only in non-deny mode, and if avoid-monitor attributes and deny attributes are set at one time, then the deny attributes will be prior. By enabling deny mode, whitelist attributes are valid and all system default subscribers cannot access to Internet, except whitelist attributes of subscribers are configured as "release". VIP attributes are used for unified flow control over static subscribers who are set with VIP attributes. Auth-deny attributes are used for setting the deny attributes of the account, which will only be valid when internal authentication is enabled. By the configuration, the account cannot access Internet and the online subscribers using this account will be forced to go off line. Pwd-edit attributes are used for setting authenticated change of the password attributes of the account, which will only be valid when internal authentication is enabled. By the configuration, the online subscribers using this account can have self-change of the password.

Common Errors

Failure to enable Layer 2/3 Classification results in failed identification after configuring subscribers.

The subscriber attribute was configured wrongly, resulting in failure of enabling this function.

1.4.10 Configuring VLAN Objects

Configuration Effect

Correlate VLAN with object names in layer 2/3.

Perform special action control over different VLANs.

Notes

Layer 2/3 Classification must be enabled for the validation of the VLAN-based policy.

The VLAN names must differ from each other and one VID can only match with one VLAN.

Configuration Steps

Configuring VLAN-group.

Optional.

It is used to configure VLAN on gateway and relate the name with VID.

Verification

Configure a VLAN relating to one VID and use PC of this VID to visit the external network.

Check whether the show run command contains the configuration information of the VLAN.

Check whether the flow is correctly matched with the VLAN in the layer 2/3 private flow space.

Related Commands

Configuring VLAN-group.

Command	**vlan-group** *name* **vlan** *vid-list*
Parameter Description	*name* - name of the VLAN *vid-list* - VID of the VLAN
Command Mode	Global configuration mode
Usage Guide	Layer 2/3 Classification supports object recognition based on VID, source IP address, or source MAC address or destination IP address.

Configuration Examples

Configuring VID 1 to 7 for VLAN A

Configuration Steps	Enabling Layer 2/3 Classification on gateway and configuring VLAN.
	FS# configure terminal FS(config)# vlan-group A vlan 1-7 FS(config)# end
Verification	Use the **show run** command to display whether there is the **layer23 classify enable** command in configuration file.

Common Errors

Policies based on VLAN are invalid and the switch of Layer 2/3 Classification is disabled.

1.5 Monitoring

Displaying

Description	Command
Displays network-group information.	**show network-group** [**all** | **brief** | **parent** [*name* /**root**]]
Displays all information of the subscriber.	**show subscriber** [**all** | **brief** | **parent** [*name* /**root**]]
Displays the VLAN information according to the displayed name.	**show vlan-group** [*name-str*]
Displays the information of the authenticated subscribers.	**show auth-subs** [**all** | **brief** | **parent** [*name* /**root**] | **dynamic** { **all** | **by-parent** xxx }]
Displays the status of the subs perception-free mode.	**show subs-mab state**
Displays the status of the strict verification mode.	**show layer23 strict-verification**

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs the private room debugging switch of the subscriber.	**debug subscriber proc-info**
Debugs the kernel room debugging switch of the subscriber.	**debug subscriber ker-info**
Debugs the private room debugging switch of the network.	**debug network proc-info**
Debugs the kernel room debugging switch of the network.	**debug network ker-info**

2 Configuring APP-IDENTIFY

2.1 Overview

Application identification refers to classification and identification of a network data flow based on application characteristics. APP-IDENTIFY analyzes packet payload and flow characteristics to obtain the application protocol type of the data flow. APP-IDENTIFY provides other functional modules (for example, flow control and flow audit) with application class information and serves as a basic module on the egress gateway.

At present, APP-ROUTE distributes application traffic depending on the initial packet identification technology. For the TCP flow, due to a lack of payload in the handshake packet, initial packet identification cannot be implemented based on the Deep Packet Inspection (DPI) rule.

2.2 Applications

Application	Description
Egress Gateway Deployment	Deploys APP-IDENTIFY on the egress gateway.

2.2.1 Egress Gateway Deployment

Scenario

An egress gateway can connect to lines of different operators, for example, one fiber line of China Telecom and one Asymmetric Digital Subscriber Line (ADSL) of China Unicom, or one fiber line of China Telecom and multiple ADSLs of China Unicom.

Functions that rely on APP-IDENTIFY include:

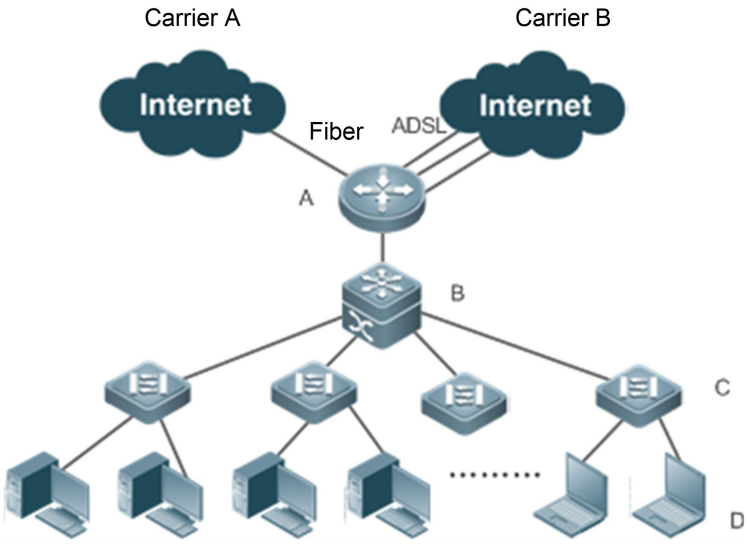
Flow control

Flow audit

Application routing

Content audit

Figure 2- 1 Typical Application Scenario of Egress Gateway



Remarks	A indicates an egress gateway. B indicates a core switch. C indicates an access switch. D indicates an intranet PC.

Deployment

Basic NAT: Implement basic network address translation (NAT) to ensure that clients access the Internet normally.

Application identification: Identify the application with traffic forwarding, and cooperate with the flow control module to implement application-based flow control.

Application routing: Enable traffic of heavy-traffic applications or key applications to be transmitted via specified egress ports based on APP-IDENTIFY.

Multi-link load balancing: Distribute traffic of data flows to multiple links to ensure proper utilization of bandwidth.

Flow control: Implement rate limitation on P2P download traffic and realize functions such as traffic guarantee of key applications in combination with APP-IDENTIFY.

Flow audit: Provide application-based traffic reports in combination with APP-IDENTIFY, so that users can learn whether the egress bandwidth is sufficient and whether capacity expansion is needed.

2.3 Features

Basic Concepts

➘ Data Flow

A data flow is a flow of packets with the same 5-tuple. According to protocols, data flows fall into three types: TCP flow, UDP flow, and IP flow (specific for non-TCP/UDP applications). The following table describes the 5-tuple of different data flows:

Flow Type	5-tuple Identifier
TCP flow	Source IP address|destination IP address|IP|TCP source port|TCP destination port
UDP flow	Source IP address|destination IP address|IP|UDP source port|UDP destination port
IP flow	Source IP address|destination IP address

➘ Application Routing

To ensure effective utilization of network resources, it is proposed that enterprises or Internet cafes rent two (or multiple) WAN links and use one high-quality line for transmitting data of key applications that are sensitive to transmission delay and jitter and use the other low-quality line for transmitting data of P2P and other download applications. To realize the method, the egress gateway should be able to route packets based on applications. Different from the conventional IP routing technology that is based on the destination IP address of a packet, application-based routing (also referred to as application routing for short) is a routing and forwarding technology that is based on application types of data flows. With the application routing technology, traffic of data flows of different application types can be distributed to different egress ports, to separate data flows of key services from data flows of rate-limited services and to minimize impact. The major problem of application routing is how to identify the initial packet of data flows. For details about application routing, refer to relevant descriptions.

➘ Initial Packet Identification

The capability of identifying the first packet of each flow is initial packet identification. This function ensures the application routing effect. If packet identification starts from the midway of a data flow, the flow will be transmitted along at least two lines, which will cause flow interruption. For the TCP flow, the initial packet is a handshake packet, and the first payload packet is a request packet.

Overview

Feature	Description
Signatures Database Upgrade	Upgrades the signatures database of the gateway.
Application Protocol Object Management	Manages application protocol objects.
APP-IDENTIFY	Identifies the application with traffic forwarding, and cooperates with the flow control module to implement application-based flow control.

2.3.1 Signatures Database Upgrade

As software is upgraded, packet characteristics of the software may change. With signatures database upgrade, packet characteristics are updated to ensure accurate and effective application identification without software upgrade.

Working Principle

The professional signatures database analysis team of FS Networks formulates a mature characteristics analysis procedure. According to the procedure, the team analyzes packet characteristics of different applications and constantly updates the characteristics to the signatures database.

Users can download the signatures database from the provided URL or obtain the signatures database from the customer service center and then upgrade the local signatures database on a Web portal. Alternatively, the signatures database can be automatically updated to the latest version via Web settings from the FS signatures database server, which is convenient and ensures automatic and timely update.

Signatures database upgrade is a procedure of analyzing and processing the compressed signatures database package (app_signature.upd) to form matching rules relevant to application identification.

After the signatures database is upgraded successfully, APP-IDENTIFY will store the signatures database to the flash memory. After the gateway restarts, the signatures database in the flash memory is automatically upgraded.

Related Configuration

Upgrading Signatures Database

By default, APP-IDENTIFY starts to parse the signatures database in the flash memory one minute after the signatures database is loaded.

Run the show identify-application version command to display the current version of the signatures database.

If the upgrade fails, the gateway uses the original signatures database. If the signatures database does not exist in the flash memory after the module performs uploading, the signatures database fails to be parsed. If the gateway does not have a signatures database, APP-IDENTIFY cannot identify any application (including user-defined applications), because there is no rule. Ensuring the latest signatures database of the gateway will improve the accuracy of application identification.

2.3.2 Application Protocol Object Management

By grouping application protocol objects, application protocol object management is simplified. By defining applications, users can define application protocol objects according to the 5-tuple information and add the user-defined application protocol objects into

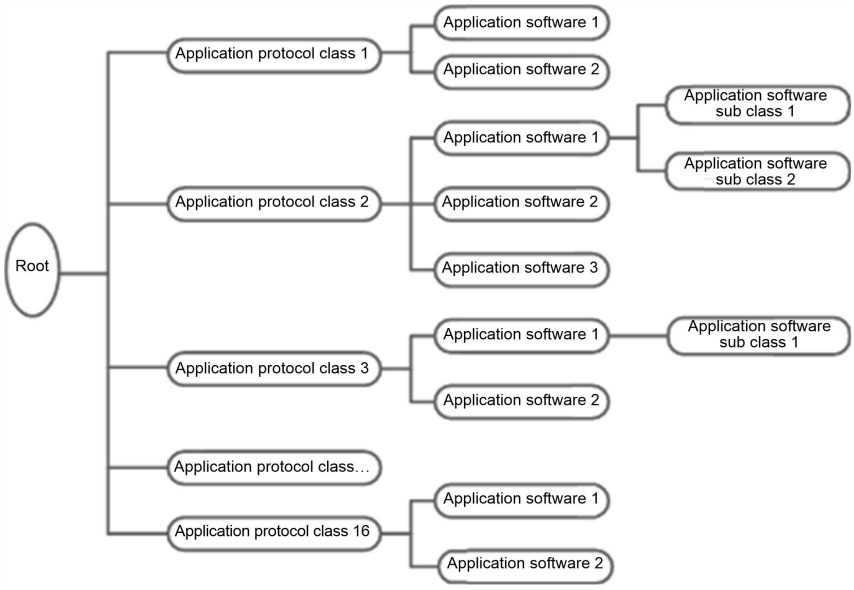
groups for management.

Working Principle

➘ Protocol Objects of Signatures Database

By parsing the signatures database, class objects are generated and a protocol tree is formed. Figure 2- 1 shows the organization form.

Figure 2- 2 Protocol tree



Applications are organized at three levels (application protocol class, application software, and application software sub class) to form a protocol tree in the system.

User-defined Application

Packets compliant with specific 5-tuple attributes are defined as one type of user-defined application.

Matching of user-defined applications is dedicated for TCP, UDP, and IP packets. Users extract the source and destination IP addresses, source and destination ports, and protocol ID from packets and query the data structures of the user-defined applications to determine whether there is a matched user-defined application.

User-defined applications are added to the same tree as other applications. The entire system has only one protocol tree, which contains all applications, including user-defined applications.

Application Grouping

According to the default classes of the system, applications are classified into the following types: instant messaging, VoIP, network game, video streaming, P2P, stock, Internet file transfer, email, database, network management protocol, routing protocol, security protocol, tunnel application, remote access protocol, network application update, online banking, network hard disk, software update, mobile Internet downloader, mobile Internet video/audio, mobile Internet web disk, mobile Internet software update, mobile Internet instant messaging, mobile Internet game, mobile Internet social network, mobile Internet web browsing, mobile Internet stock, and RFC.

First grouping mode: According to the preset groups of the system, applications are classified into the following four groups: key application group, rate-limited application group, blocked application group, IP protocol group. The names of these application groups cannot be modified, but users can add the default application group of the system or an application of a group into the above four groups.

Second grouping mode: Applications can be grouped according to user requirements as well. Users can add the default application groups of the system or an application of a group into the custom group.

Related Configuration

Displaying Applications and Application Groups

Run the show identify-application command to display current application tree, including application protocol objects parsed out from the signatures database and user-defined applications.

Run the show identify-application custom-group command to display group information.

Defining Applications

By default, no application is defined by users.

User-defined applications fall into the following types:

21. Protocol type and source and destination ports
22. Protocol type, source IP address, and source port
23. Protocol type and source and destination IP addresses
24. Protocol type, destination IP address, and destination port

Run the identity-application custom name command to define applications. Pay attention to the following limits during configuration:

For the first type of applications, the source and destination ports cannot be set to any at the same time.

For the second type of applications, neither the source IP address nor the source port can be set to any.

For the third type of applications, the source and destination IP addresses cannot be set to any at the same time.

For the fourth type of applications, neither the destination IP address nor the destination port can be set to any.

A single IP address or an IP address segment can be configured. In the IP address segment, the number of IP addresses cannot be greater than 32 and the IP addresses must be consecutive.

Users can add applications to an existing class or add characteristics to an existing application. In other cases, the name of a user-defined application should not be the same as that of an existing application or class.

The name of a user-defined class contains no more than 31 characters, and the name of a user-defined application contains no more than 27 characters.

Grouping Applications

The system classifies applications based on the first grouping mode. Run the show identify-application group-state command to display current application classification mode.

Run the **identify-application clear key-inhibitive-block-other group** command to clear all applications in the key application group, rate-limited application group and blocked application group. Applications are classified according to the second grouping mode.

In the first grouping mode, when an application is added into the key application group, rate-limited application group or blocked application group, the view of the second grouping mode appears. When an application is added to the custom application group, the view of the second grouping mode appears as well.

In the second grouping mode, an application, if not added to the key application group, rate-limited application group or blocked application group, belongs to the IP protocol group by default. If it is added to the key application group/rate-limited application, it belongs to the key application group/rate-limited application.

In the second grouping mode, default applications or application groups can be added to multiple custom groups. For example, the email protocol application can be added to User-defined Group 1 and User-defined Group 2 at the same time.

In the first grouping mode, run the identify-application block, identify-application inhibitive, identify-application key to add an application or an application group to the blocked application group, rate-limited group and key application group respectively.

Run the identify-application custom-group command to create a group, enter the application group configuration mode after the group is created, and then run the app-add or app-del command to add or delete applications or application classes.

An application cannot be added to the key application group and rate-limited application group at the same time, but the application and corresponding application group can be added to different system groups. For example, for Tencent QQ (a type of

instant messaging software) and the group of instant messaging software, the group of instant messaging software can be added to the key application group while Tencent QQ is added to the rate-limited application group. Without manual intervention, Tencent QQ will be added to the same system group (that is, the key application group) as the group of instant messaging software by default.

Application identification protocols fall into custom protocols and signatures database protocols. The user-defined protocols prevail over the signatures database protocols. If a protocol is custom by users and also exists in the signatures database, the system prefers the custom protocol.

A maximum of 100 application groups can be defined.

2.3.3 APP-IDENTIFY

APP-IDENTIFY identifies application attributes of data flows so that other modules execute policy actions according to the application attributes.

Working Principle

APP-IDENTIFY identifies the application attributes of data flows using technologies such as predictive identification, DPI, detective identification, Deep/Dynamic Flow Inspection (DFI), and length sequence identification.

Predictive Identification

Some application protocols have distinct flow characteristics. For example, a flow may contain information such as an IP address and a port for subsequent sessions. With an analysis on the flow information, flow characteristics are extracted and recorded. Subsequent flows that comply with the characteristics can be identified as flows of the application. The predicted characteristics will age after a period of time. Users can configure the aging time.

Detective Identification

Some application protocols may generate unknown encrypted data flows. The FS gateway can identify the application type corresponding to this type of encrypted data flows using detection mechanisms.

DPI

DPI is specific for payloads of packets. By parsing the packet payloads based on the protocol layer, the DPI identifies the protocol type and port of the packets, encodes the payloads, and then matches the payload content with the strings in the signatures database. Multiple models are used to match and identify the payload characteristics. If different match results are obtained, the DPI selects a final result based on priorities. If the protocol type of an application has to be determined by identifying payloads of multiple packets, the status tracking module will trace the status.

DFI

DFI is a technology that identifies applications based on flow characteristics. Generally, session connections or data flow statuses vary with the specific application type, for example, the P2P download flow and voice flow. DFI identifies the characteristics of the data flows, builds flow classifiers, and then classifies the data flows using the classifiers, thereby implementing smart identification of application types.

Length Sequence Identification

Packet payloads generated by some applications, though encrypted, feature a fixed length. Based on this characteristic, encrypted P2P

download flows can be identified. A typical example is the eDonkey encrypted download flow.

Related Configuration

Enabling APP-IDENTIFY

The module is enabled by default.

Run the identify-application enable command to enable the module.

The identification functions above can take effect only after the module is enabled. In this case, each function can be disabled separately.

Enabling Predictive Identification

The predictive identification function is enabled by default provided that APP-IDENTIFY is enabled.

Run the identify-application proto-expect enable command to enable predictive identification.

If predictive identification is disabled, the identification capability of the system may be reduced greatly. Generally, it is not recommended to disable predictive identification.

For the protocol information that is obtained by dynamic analysis, aging time must be specified. If such aging time is not specified, the default aging time of the system is used.

The aging time of protocol information is 60 seconds by default.

Run the identify-application proto-expect timeout command to configure aging time of protocol information.

A longer aging time indicates longer protocol information TTL. Generally, the default aging time is used. If the aging time is set to a great value, the predictive identification capability may be improved, which however is likely to cause misjudgment.

Enabling DPI

The DPI function is enabled by default provided that APP-IDENTIFY is enabled.

Run the identify-application dpi enable command to enable DPI.

If DPI is disabled, the identification capability of the system may be reduced greatly. Generally, it is not recommended to disable DPI.

Enabling Length Sequence Identification

The length sequence identification function is enabled by default provided that APP-IDENTIFY is enabled.

Run the identify-application len-seq enable command to enable length sequence identification.

If length sequence identification is disabled, the identification rate of the encrypted P2P flow may be reduced. Generally, it is not recommended to disable length sequence identification.

2.4 Configuration

Configuration	Description and Command	
Upgrading Signatures Database	(Mandatory) It is used to build a protocol tree and rules of the signatures database.	
	Identify-application signature update	Triggers signatures database upgrade.
Defining Applications	(Optional) It is used to define application rules.	
	identity-application custom name	Defines application rules.
Grouping Applications	(Optional) It is used to manage application protocol objects.	

	identify-application clear key-inhibitive-block-other group	Clears all the applications in the key application group, rate-limited application group, and blocked application group.
	identify-application custom-group	Defines a group.
	app-add	Adds applications to the user-defined group.
	app-del	Deletes applications from the user-defined group.
	identify-application block	Blocks applications from the user-defined group.
	identify-application key	Adds an application to the key application group.
	identify-application inhibitive	Adds an application to the rate-limited application group.
Configuring APP-IDENTIFY	(Mandatory) It is used to enable APP-IDENTIFY.	
	identify-application enable	Enables APP-IDENTIFY.
	identify-application proto-detect enable	Enables detective identification.
	identify-application proto-expect enable	Enables predictive identification.
	identify-application proto-expect timeout	Sets aging time of protocol information.
	identify-application dpi enable	Enables DPI.
	identify-application dfi enable	Enables DFI.
	identify-application len-seq enable	Enables length sequence identification.
	identify-application app-db enable	Enables the application collection function.

2.4.1 Upgrading Signatures Database

Configuration Effect

Build a protocol tree of the signatures database.

Create or update the signatures database rules.

Notes

If the current database version of the gateway is consistent with the target database version, the upgrade fails.

Configuration Steps

Upgrading Signatures Database

Mandatory.

Upgrade the signatures database on the egress gateway. Obtain the signatures database from the official website to the local PC, download the compression package of the signatures database to the gateway, and then upgrade the local signatures database on the

web portal. Alternatively, the signatures database can be updated in HTTP mode.

For details about HTTP upgrade, refer to relevant documents. This document mainly describes the configuration method of local upgrade. If the upgrade is implemented via a web portal or automatic update, users do not need to run relevant commands to trigger signatures database parsing.

Verification

Check the version number of the signatures database to determine whether the signatures database is upgraded successfully.

Related Commands

Upgrading Signatures Database

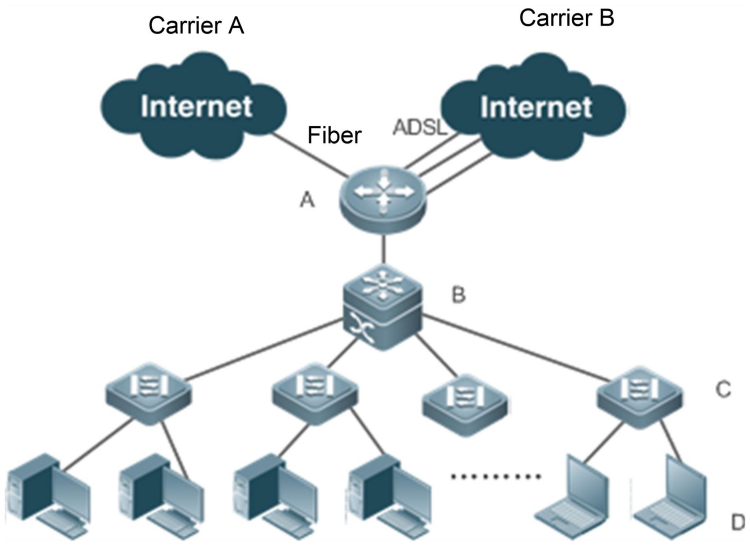
Command	**Identify-application signature update**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Download the compression package of the signatures database to the gateway and run this command to trigger signatures database upgrade.

Displaying Version Number of Signatures Database

Command	**show identify-application version**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	N/A

Configuration Example

Upgrading Signatures Database

Scenario **Figure 2–3**	
Configuration Steps	● Choose **Advanced** > **System Upgrade** > **Signatures Database Download** > **Download Application Database** to download the signatures database package to the gateway. ● Decompress the package, choose **Advanced** > **System Upgrade** > **Local Upgrade** to select the **app_signature.upd** file in the package directory, and click **Start** to upgrade the signatures database. The system will prompt upgrade success after the upgrade.
A	FS#*Apr 25 14:08:55: %DPI-5-LOCAL_UPDATE: Local signature database upgrading. FS#*Apr 25 14:10:14: %DPI-5-SIGNATURE_UPDATE: Signature database is upgraded successfully!
Verification	● Run the **show identify-application version** command to display the version number of the signatures database.
A	FS#show identify-application version Version:2013.05.22.13.05.22(V2.0)

Common Errors

The current database version of the gateway is consistent with the target database version.

2.4.2 Defining Applications

Configuration Effect

Define applications and identify application traffic based on the 5-tuple information.

If the gateway does not have a signatures database, user-defined applications cannot be identified.

Notes

User-defined applications fall into the following types:

Protocol type and source and destination ports

Protocol type, source IP address, and source port

Protocol type and source and destination IP addresses

Protocol type, destination IP address, and destination port

Pay attention to the following limits during configuration:

For the first type of applications, the source and destination ports cannot be set to any at the same time.

For the second type of applications, neither the source IP address nor the source port can be set to any.

For the third type of applications, the source and destination IP addresses cannot be set to any at the same time.

For the fourth type of applications, neither the destination IP address nor the destination port can be set to any.

A single IP address or an IP address segment can be configured. In the IP address segment, the number of IP addresses cannot be greater than 32 and the IP addresses must be consecutive.

Users can add characteristics to an existing application or application class. The original characteristics of the existing application or application class are not affected but are less prioritized than the user-defined application characteristics.

The name of a user-defined class contains no more than 31 characters, and the name of a user-defined application contains no more than 27 characters.

If user-defined applications share a source or destination IP address, a maximum of 16 port configurations can be configured for the applications. For example, for the combination of destination IP address + destination port, the possible configurations are IP:1.1.1.1 + port:80, IP:1.1.1.1 + port:100, and IP:1.1.1.1 + port:200.

Configuration Steps

Run relevant commands in global configuration mode to create applications.

Verification

Check whether the user-defined applications are created successfully.

Related Commands

Defining Rules

Command	**identity-application custom name** *software-name* **class** *class-name* **{ ip sip { any any |** *sip-low sip-high* **} dip { any any |** *dip-low dip-high* **} | { tcp | udp } { sport { any any |** *sport-low sport-high* **} dport { any any |** *dport-low dport-high* **} | { sip { any any |** *sip-low sip-high* **} { sport { any any |** *sport-low sport-high* **} | dip { any any |** *dip-low dip-high* **} } | dip { any any |** *dip-low dip-high* **} dport { any any |** *dport-low dport-high* **} } } }**
Parameter Description	software-name: Indicates an application name. class-name: Indicates an application class name. sport-low: Indicates the start source port. The value ranges from 0 to 65,535 or is **any**. sport-high: Indicates the end source port. The value ranges from 0 to 65,535 or is **any**. dport-low: Indicates the start destination port. The value ranges from 0 to 65,535 or is **any**. dport-high: Indicates the end destination port. The value ranges from 0 to 65,535 or is **any**. sip-low: Indicates the start source IP address. sip-high: Indicates the end source IP address. dip-low: Indicates the start destination IP address. dip-high: Indicates the end destination IP address.
Command Mode	Global configuration mode
Usage Guide	N/A

Displaying Defined Rules

Command	**show identify-application custom- rule**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Example

Defining Rules

Configuration Steps	● Define a rule.
	FS# configure terminal FS(config)#identify-application custom name XLgame class Custom Game tcp sport 1 10 dport 1 100
Verification	● Display the defined rule on the gateway.
	FS#show identify-application custom-rule TYPE NAME CLASS SPL SPH DPL DPH SIPL SIPH DIPL DIPH ---- ---------- ---------- ----- ----- ----- ----- ---------- ---------- ---------- ---------- TCP XLgame Custom Game 1 10 1 100 any any any any

Common Errors

The specified limit conditions are not met. For details about the limit conditions, refer to the preceding Notes.

2.4.3 Grouping Applications

Configuration Effect

Group applications so that the flow control and application routing modules can associate policies with the application groups.

Notes

An application cannot be added to the key application group and rate-limited application group at the same time, but the application and corresponding application group can be added to different system groups. For example, for Tencent QQ (a type of instant messaging software) and the group of instant messaging software, the group of instant messaging software can be added to the key application group while Tencent QQ is added to the rate-limited application group. Without manual intervention, Tencent QQ will be added to the same system group (that is, the key application group) as the group of instant messaging software by default.

Application identification protocols fall into custom protocols and signatures database protocols. The user-defined protocols prevail over the signatures database protocols. If a protocol is custom by users and also exists in the signatures database, the system prefers the custom protocol.

A maximum of 100 application groups can be defined.

Configuration Steps

Decide a grouping mode.

Create groups.

Add applications or application classes to the groups.

Verification

Check the current application grouping mode.

Display groups and confirm that the groups are created successfully.

Display the applications or application classes in the groups.

Related Commands

Configuring Grouping Mode

Command	**identify-application clear key-inhibitive-block-other group**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to delete applications from system groups.

Creating Groups

Command	**identify-application custom-group** *group-name*
Parameter Description	group-name: Indicates a group name.
Command Mode	Global configuration mode
Usage Guide	Use this command to add user-defined groups. A maximum of 100 classes of application groups can be defined. After the command is run, enter the group-group mode.

Adding Applications to Groups

Command	**app-add** *app-name*
Parameter Description	app-name: Indicates an application name.
Command	application group configuration mode

Mode	
Usage Guide	Use this command to add applications (including applications and application classes) to the groups.

Deleting Applications from Groups

Command	**app-del** *app-name*
Parameter Description	app-name: Indicates an application name.
Command Mode	application group configuration mode
Usage Guide	Use this command to delete applications from the groups.

Configuring Blocked Application Group

Command	**identify-application block** *app-name*
Parameter Description	app-name: Indicates an application name.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Key Application Group

Command	**identify-application key** *app-name*
Parameter Description	app-name: Indicates an application name.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Rate-limited Application Group

Command	**identify-application inhibitive** *app-name*
Parameter Description	app-name: Indicates an application name.
Command Mode	Global configuration mode
Usage Guide	N/A

Displaying Protocol Tree

Command	**show identify-application**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying Application Classes

Command	**show identify-application class [class-name]**
Parameter Description	**class-name**: Indicates a class name.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying Current Application Grouping Mode

Command	**show identify-application group-state**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying Groups and Applications or Application Classes in Groups

Command	**show identify-application custom-group**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying Blocked Application Group

Command	**show identify-application block**
Parameter Description	N/A

Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying Key Application Group

Command	**show identify-application key**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying Rate-limited Application Group

Command	**show identify-application inhibitive**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying Other Application Group

Command	**show identify-application other**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Example

Creating Groups and Adding Applications to Groups

Configuration Steps	● Create a group. ● In application group configuration mode, add applications to the group.
	FS# configure terminal FS(config)#identify-application custom-group mygroup FS(config-custom-group)#app-add BQQ FS(config-custom-group)#app-add MSN FS(config-custom-group)#exit
Verification	● Display the groups and applications in the groups.
	FS#show identify-application custom-group system-group: Key_Group system-group: Unkey_Group system-group: Block_Group application: HTTP-single thread system-group: Other_Group custom-group: mygroup application: BQQ application: MSN (group)

Configuring System Groups

Configuration Steps	● Add applications or application classes to the key application group.
	FS# configure terminal FS(config)#identify-application key BQQ
Verification	● Display the groups and applications in the groups.
	FS#show identify-application key BQQ FS#

Common Errors

The specified limit conditions are not met. For details about the limit conditions, refer to the preceding Notes.

2.4.4 Configuring APP-IDENTIFY

Configuration Effect

After APP-IDENTIFY is configured, application types of different data flows can be identified and application information can be collected.

Notes

If APP-IDENTIFY is disabled, all application identification functions are invalid.

The application identification functions rely on the signatures database. If the gateway does not have a signatures database, application identification is invalid.

The application identification functions are enabled by default provided that APP-IDENTIFY is enabled.

Configuration Steps

- In global configuration mode, run relevant commands to enable APP-IDENTIFY and application identification functions.

Verification

Check the module status and statuses of different application identification functions.

Related Commands

Enabling APP-IDENTIFY

Command	**identify-application enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling Detective Identification

Command	**identify-application proto-detect enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling Predictive Identification

Command	**identify-application proto-expect enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Setting Aging Time of Protocol Information

Command	**identify-application proto-expect timeout** *time-seconds*
Parameter Description	time-seconds: Indicates the aging time in seconds. The value ranges from 10 to 3600.
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling DPI

Command	**identify-application dpi enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling DFI

Command	**identify-application dfi enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling Length Sequence Identification

Command	**identify-application len-seq enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling Application Collection

Command	**identify-application app-db enable**
Parameter Description	N/A
Command Mode	Global configuration mode

Usage Guide	N/A

Displaying APP-IDENTIFY

Command	**show identify-application enable**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying Predictive Identification Function

Command	**show identify-application proto-expect enable**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to display the prediction status and default aging time.

Displaying DFI Function

Command	**show identify-application dfi enable**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to display the prediction status and default aging time.

Configuration Example

Enabling APP-IDENTIFY

Configuration Steps	• Enable APP-IDENTIFY. • Disable DFI.
	FS# configure terminal FS(config)#no identify-application dfi enable
Verification	• Display APP-IDENTIFY and the DFI function.

	FS#show identify-application enable on FS#show identify-application dfi enable dfi unable!

Enabling Predictive Identification

Configuration Steps	● Enable the predictive identification function. ● Enable the application collection function.
	FS# configure terminal FS(config)#identify-application proto-expect enable FS(config)#identify-application app-db enable
Verification	● Display the predictive identification function.
	FS#show identify-application proto-expect enable Proto-expect is enable Proto-expect app_db is enable Proto-expect timeout is not set[0s]

Common Errors

APP-IDENTIFY is disabled, causing enabling failure of an application identification function.

2.5 Monitoring

Displaying

Description	Command
Displays the application protocol tree information.	**show identify-application**
Displays the applications or application classes that are added to the blocked application group.	**show identify-application block**
Displays the application class information.	**show identify-application class**
Displays the application group information.	**show identify-application custom-group**
Displays the user-defined application rules.	**show identify-application custom- rule**

Displays APP-IDENTIFY.	**show identify-application enable**
Displays the grouping mode.	**show identify-application group-state**
Displays the applications or application classes that are added to the rate-limited application group.	**show identify-application inhibitive**
Displays the applications or application classes that are added to the key application group.	**show identify-application key**
Displays the applications or application classes that are added to the Other application group.	**show identify-application other**
Displays the predictive protocol information.	**show identify-application proto-expect enable**
Displays the detective protocol information.	**show identify-application proto-detect enable**
Displays the version number of the signatures database.	**show identify-application version**

3 Configuring APP-ROUTE

3.1 Overview

Different from the conventional IP routing technology that is based on the destination IP address of a packet, application-based routing (also referred to as application routing for short) is a routing and forwarding technology that is based on application types of data flows. With the application routing technology, traffic of data flows of different application types can be distributed to different egress interfaces, to separate data flows of key services from data flows of rate-limited services.

APP-ROUTE of the FS egress gateway mainly applies to the following scenario:

Because the prices of the fiber line and Asymmetric Digital Subscriber Line (ADSL) are greatly different (in some areas, the prices vary by 7 or 8 times per meter), a combination of fiber line with ADSL is used to improve the cost performance. APP-ROUTE allows clients to transfer data of rate-limited applications to the ADSL and data of key applications to the fiber line. Via such distribution, key applications can obtain better line resources to improve user experience, which ensures the optimal cost performance between the bandwidth investment cost and user experience.

3.2 Applications

Application	Description
Distributing Traffic on Multiple Egress Interfaces of NetBar Based on Application	Uses a combination of fiber line with ADSL on egress interfaces of a NetBar.

3.2.1 Distributing Traffic on Multiple Egress Interfaces of NetBar Based on Application

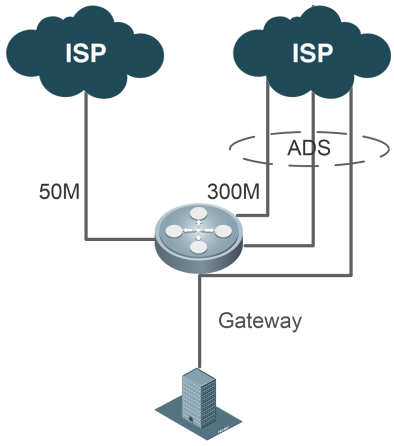
Scenario

The network platform of a NetBar run different types of services, including key applications (such as games, browsing, and instant messaging) and rate-limited applications (such as online movies and P2P download). For the NetBar, key applications are their core competitive edge, and rate-limited applications are less important.

According to the Figure 3- 1, China Telecom provides one fiber line and three ADSLs for the NetBar.

For NetBar clients, it must be ensured that data of key applications is transferred along the fiber line, while data of rate-limited applications (such as video and download) is transferred along the ADSLs.

Figure 3- 1



Deployment

Enable APP-ROUTE.

Configure routing policies for the web application.

Configure routing policies for the video application.

Configure routing policies for the rate-limited applications such as P2P. Generally, ADSLs are recommended.

Configure the interface group function.

3.3 Features

Basic Concepts

Application Identification

Application identification indicates identification of a network data flow based on application characteristics in order to obtain the application protocol type of the data flow. APP-IDENTIFY analyzes packet payload and flow characteristics to obtain the application protocol type of the data flow. The analysis result serves as the basis for packet forwarding by APP-ROUTE.

Application Class

APP-ROUTE matches and distributes traffic of data flows according to the configured application classes. It supports application class, application software, application software sub class, and application group.

Different from the preceding three items, the application group can be considered a container. Users can distribute application classes, application software, and application software sub classes to the group. The predefined system groups include the key application group, rate-limited application group, blocked application group, and other application group. Users can define new application groups. With APP-ROUTE, routes can be specified for all the application groups.

The application class, application software, and application software sub class are in hierarchical relationships. An application class contains several types of software, and a type of software contains no or several software sub classes. A large number of application classes, application software, and application software sub classes have been predefined in the signatures database. For example, the HTTP application class contains the HTTP video streaming media software that contains Youku videos and Tudou videos. Youku can be considered a subset of the HTTP video streaming media software, and the HTTP video streaming media software can be considered a superset of Youku. In addition to the predefined classes, users can define new classes, software, and sub classes. The following table lists the application classes, application software, and application software sub classes supported by APP-ROUTE.

Application Class	Application Software	Application Software Sub Class	APP-ROUTE
P2P download	(All)	(All)	Y
Video streaming	(All)	(All)	Y
HTTP	HTTP video streaming	(All)	Y
Network application update	(All)	(All)	Y
Network disk	(All)	(All)	Y
Internet file transmission (including IM file)	(All)	(All)	Y

If APP-ROUTE supports an application class, it supports the software and software sub classes under this class. However, if APP-ROUTE supports the software or software sub class, it does not necessarily support the application class. For example, APP-ROUTE supports the HTTP video streaming media software and its sub classes, but it does not support the HTTP application

class. APP-ROUTE supports user-defined groups. If a user-defined group contains an application class that does not support initial packet identification, traffic of the data flows of the application class may not be properly distributed.

For details about the application class, application software, and application software sub class supported by APP-ROUTE, refer to the SRS or web description.

#if defined (CONFIG_EG_URL_ROUTE)

UrlURL-group

APP-ROUTE can distribute traffic according to the URLs in the DNS request packets. The url-group is a group of specific URLs and can be defined by users or generated by the system by default. For example, the default url-group video~sys of the gateway contains common URLs of video websites, for example, k.youku.com. This function is specific to DNS request packets and requires cooperation from the DNS proxy. During url-group configuration, users can determine whether to change the destination IP addresses in the DNS request packets.
#endif

Priority

Different routing technologies, including application routing, IP routing, user-based routing, policy-based routing, and default routing can serve as the basis for packet forwarding. The priorities of the routing technologies are as follows:
Policy-based routing (set ip nexthop) > User-based routing > Application routing > IP routing > Policy-based routing (set ip default nexthop) > Default routing
If multiple application routes coexist, they are used according to priorities as well.
The priorities of application routes are correlated to the configuration sequence. The application route configured later prevails over the application route configured earlier.

Hit

A hit indicates that a data flow matches a routing policy and traffic of the data flow is forwarded according to the policy. Because APP-ROUTE is characterized by initial packet identification, data flows of applications that do not support initial packet identification do not hit any policy of APP-ROUTE.

Status

The status of an application route, also referred to as activeness, indicates that whether the application route takes effect. If the egress interface of the application route is in the Down state, the application route is in the Down state as well.
If APP-ROUTE is disabled, all application route policies are in the Down state.

Interface and interface group

The egress interface of an application route can be a WAN interface.
An interface group is a combination of multiple WAN interfaces. This concept is defined to support multilink routing and simplify configuration. Users can specify names for an interface group, including interface members and balancing policies.
The egress interface of an application route can be an interface or interface group.

IP Group Address Table

The source or destination IP address can be used as a basis of application routing. Users can define different addresses, including URLs, IP addresses, and IP masks in an IP group.
After the source or destination IP address is specified, traffic with the source or destination IP address matching the specified address will

be routed based on application routing.

If the application type is specified as any, application routes with the destination IP addresses being the address of the Telecom address library can be configured as an address library of China Telecom.

If the application type is specified as any, application routes with the source IP addresses being the intranet server address can be configured as policy-based routes.

↘ IP Protocol ID and Port Range

APP-ROUTE supports a specified IP protocol and specified ranges of the source and destination ports when the TCP or UDP is selected. Only traffic complying with the protocol and the port ranges can hit the policy. When the application routing policy is associated with information such as an object group and an IP addresses list, traffic hits the policy only when the traffic matches all the associated information.

Overview

Feature	Description
Configuring Application Routing	Distributes and processes traffic according to the application routing policies.
Configuring Interface Group	Combines multiple egress interfaces so that APP-ROUTE can select routes based on the egress interfaces.

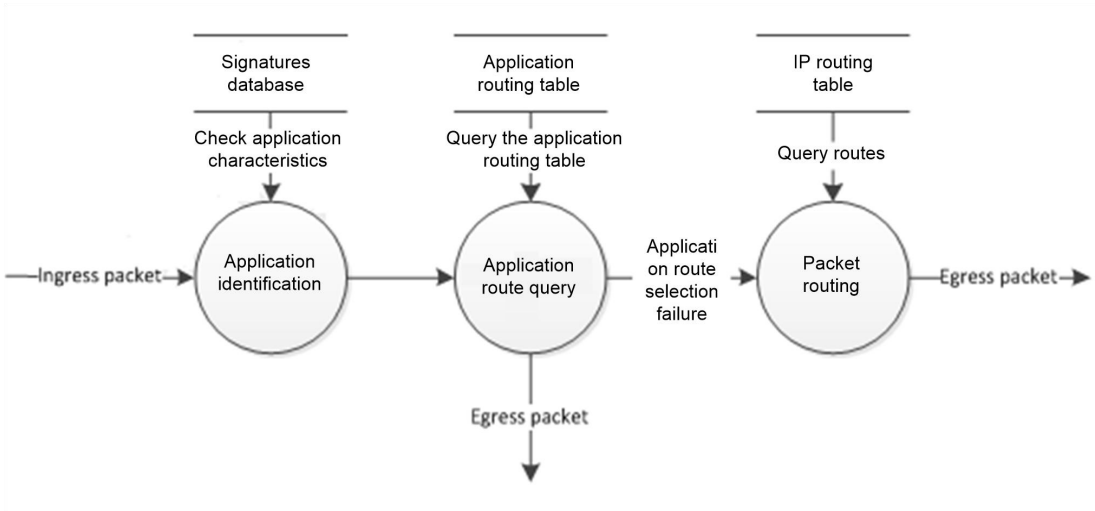
3.3.1 Configuring APP-ROUTE

Configure application routing policies to distribute and process traffic of applications on the egress interfaces.

Working Principle

Similar to common IP routing, APP-ROUTE has an application routing table. If a data flow is generated, APP-IDENTITY analyzes packets of the data flow to determine its application type. When receiving the packets, APP-ROUTE queries the application routing table to determine the next hop and egress interface and forwards the packets, as shown in Figure 3- 2. If no entry is hit, the packets are forwarded according to common IP routing.

Figure 3- 2



Application Routing Table

The application routing table records information about packets that comply with application routing policies, mainly including egress interface and next hop information.

Related Configuration

Enabling APP-ROUTE

APP-ROUTE is disabled on the FS gateway by default.

In global configuration mode, run the app-route enable command to enable APP-ROUTE.

In global configuration mode, run the no app-route enable command to disable APP-ROUTE.

Configuring APP-Route

No policy is configured on the gateway by default.

Run the app route [priority-num priority-num] app-name [protocol {tcp [sport s-begin [s-end]] [dport d-begin [d-end]] | udp [sport s-begin [s-end]] [dport d-begin [d-end]] | icmp | protocol-num}] [sip-group sip-group-number] [dip-group dip-group-number] [url-group url-group-name [change-dest dest-ip-address]] {interface interface-name | interface-group group-name} [time-range time-rang-name] [track track-id] [description description-name] command to configure application-based routes..

Packet matching rules are specified by the keywords app-name, sip-group-number, dip-group-number, and url-group-name.

Processing methods of packets that match the rules are specified by the keywords dest-ip-address, interface, and interface-group.

Rules that are not entered will not be used by default.

After policies are configured and application routes take effect, data packets will be distributed and processed according to applications.

Policies configured later prevail over policies configured earlier. Users can run relevant commands to change the priorities of policies.

Changing Priorities of Policies

By default, policies configured later prevail over policies configured earlier.

In global configuration mode, run the app route priority-num priority-number priority { increase | decrease } [1-1999] command to change the priorities of policies.

Policies with higher priorities will be matched first.

Application routes can be used in gateway mode, but not bridge mode.

3.3.2 Specifying Source/Destination IP Address

APP-ROUTE can route packets according to specified source/destination IP address. By configuration of the IP address associated with the IP group (for details, see the configuration document about the IP group), APP-ROUTE associates with the IP group and routes packets to the specified egress interface.

Related Configuration

Configuring IP Group

In global configuration mode, configure an IP address range using the IP group function.

Configuring Policies

In global configuration mode, run the priority priority-num app-name [protocol { tcp [sport s-begin [s-end]] [dport d-begin [d-end]] | udp [sport s-begin [s-end]] [dport d-begin [d-end]] | icmp | protocol-num }] [sip-group sip-group-number] [dip-group dip-group-number] [url-group url-group-name [change-dest dest-ip-address]] [time-range time-rang-name] [static-route]

[description description-name]app route app-name [sip-group sip-group-number] [dip-group dip-group-number] [url-group url-group-name [change-dest dest-ip-address]] { interface interface-name | interface-group group-name} [time-range time-rang-name] [track track-id] [static-route] [description description-name] command to configure policies for application routing.

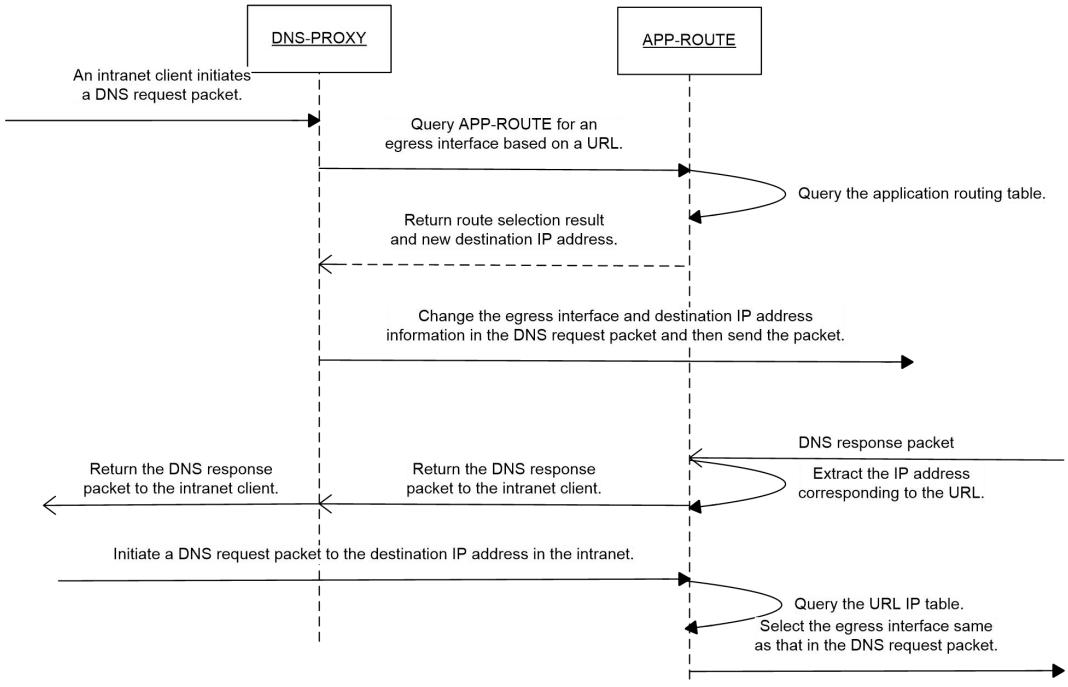
3.3.3 Configuring URL-based Route

APP-ROUTE can route packets according to specified URL. By configuration of the URL associated with the IP group (for details, see the configuration document about the IP group), APP-ROUTE associates with the IP group and routes packets to the specified egress interface.

Working Principle

During url-group configuration, APP-ROUTE is used in combination with the DNS proxy function. The DNS request packets are processed by the DNS proxy, and APP-ROUTE provides the routing table and processes the IP address after the DNS is resolved.
For example, an intranet PC initiates a DNS request packet with the URL being k.youku.com. The DNS proxy intercepts the packet, extracts the URL information, and queries APP-ROUTE. After detecting that the URL is in the default system group video~sys and Egress Interface 1 has been specified for url-group, APP-ROUTE returns Egress Interface 1 to the DNS proxy. The DNS proxy routes the packet to Egress Interface 1. When receiving a DNS response packet from the extranet DNS server, APP-ROUTE intercepts the packet, extracts the IP address corresponding to the URL, and caches the IP address, for example, 119.167.145.107 corresponding to k.youku.com, to the URL IP table. If the destination IP address in subsequent DNS request packets matches this IP address, APP-ROUTE redirects the DNS request packets to Egress Interface 1.

Figure 3- 3



The destination IP address in a DNS request packet can be modified.

Related Configuration

- **Configuring IP Group**

In global configuration mode, run the app-proxy url group url-group-name command to specify a URL.

Configuring Policies

In global configuration mode, run the app route app-name [sip-group sip-group-number] [dip-group dip-group-number] [url-group url-group-name [change-dest dest-ip-address]] { interface interface-name | interface-group group-name} [time-range time-rang-name] [track track-id] command to configure policies for application routing.

3.3.4 Configure Interface Group

Combine multiple egress interfaces to form an interface group.

Working Principle

An interface group can contain a maximum of 32 interfaces. Each interface member is an egress interface. Different line load policies can be configured for the interface group. For an interface group based on the bandwidth policy, interface members are weighed according to bandwidth. For an interface group based on the load policy, bandwidth utilization rates are updated by a load interval and the minimum load is calculated.

Calculating Bandwidth Weight

Supposed that the total bandwidth of the interface group is S, bandwidth of each egress interface is Bi, base weight is base, and weight value is Wi, the weight value is calculated according to the following formula:

$Wi = Bi \times base / S$

Related Configuration

Configuring Interface Group

No interface group is configured on the gateway by default.

In global configuration mode, run the interface-group interface-group-name command to configure objects of an interface group.

In global configuration mode, run the no interface-group interface-group-name command to delete objects from an interface group.

Configuring Interface Members

No interface member is configured in an interface group by default.

In interface configuration mode, run the interface-member interface-name command to configure interface members.

In interface configuration mode, run the no interface-member interface-name command to delete interface members.

Configuring Load Policy

An interface group balances load based on lines by default.

In interface configuration mode, run the load-balance policy { bandwidth | load } command to configure a load policy.

The parameter bandwidth indicates line-based bandwidth, and the parameter load indicates line-based load.

The default load policy of the interface group is line-based bandwidthload.

Configuring Interface Gateway

No next hop is configured on an interface by default.

In interface configuration mode, run the nexthop ip-address command to configure the next hop of the interface.

The interface gateway function is configured for the interface members in the group.

3.4 Configuration

Configuration	Description and Command	
Configuring APP-ROUTE	(Mandatory) It is used to validate application routing policies and distribute and process traffic of applications complying with the policies.	
	app-route enable	Enables APP-ROUTE.
	app route [**priority-num** *priority-num*] *app-name* [**protocol** {**tcp** [**sport** *s-begin* [*s-end*]] [**dport** *d-begin* [*d-end*]] | **udp** [**sport** *s-begin* [*s-end*]] [**dport** *d-begin* [*d-end*]] | **icmp** | *protocol-num*}] [**sip-group** *sip-group-number*] [**dip-group** *dip-group-number*] [**url-group** *url-group-name* [**change-dest** *dest-ip-address*]] {**interface** *interface-name* | **interface-group** *group-name*} [**time-range** *time-rang-name*] [**track** *track-id*] [**description** *description-name*]]	Configures APP-ROUTE.
	nexthop *ip-address*	Configures the gateway.
	(Optional) It is used to change priorities of application routing policies.	
	app route priority-num *priority-number* **priority** { **increase** | **decrease** } [*1-1999*]	Configures priorities of application routing policies.
Configuring Interface Group	(Mandatory) It is used to configure basic information of an interface group.	
	interface-group *interface-group-name*	Configures the name of an interface group.
	interface-member *interface-name*	Adds interfaces to the group.
	nexthop *ip-address*	Configures the interface gateway function.
	(Optional) It is used to configure advanced information of an interface group.	
	load-balance policy { **bandwidth** | **load** }	Configures load policies.
	bandwidth *kilobits*	Configures interface bandwidth.

3.4.1 Configuring APP-ROUTE

Configuration Effect

Validate application routing policies, and distribute and process traffic of applications complying with the policies.

Notes

The gateway IP address must be configured on interfaces.

Application objects must support initial packet identification.

url-group must be enabled under the support of a DNS proxy.

The time-range object associated with application routing must be validated.

Configuration Steps

Enabling APP-ROUTE

Mandatory.

Control APP-ROUTE through a global switch.

Configuring Policies

Mandatory.

In global configuration mode, configure policies and determine the applications that apply application routingthe policy name.

Configure priority, application, IP object, URL object and time object.

Correlate an interface/interface group or SLA with an application route policy.

Configuring Interface Gateway

Mandatory.

Configure the gateway function on WAN interfaces only.

Configuring Priorities of Policies

Optional. Use this function when the priorities of policies need to be changed.

Policies configured later prevail over policies configured earlier. With this function, priorities of policies can be changed.

Verification

Check whether data packets of application objects that match an application routing policy are distributed and processed according to application routing.

Check whether application objects are distributed and processed through the specified egress interface.

Check whether the configuration of APP-ROUTE takes effect.

Display the statistics about egress interfaces of application routing.

Related Commands

Enabling APP-ROUTE

Command	**app-route enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring APP-ROUTE

Command	**app route** [**priority-num** *priority-num*] *app-name* [**protocol** {**tcp** [**sport** *s-begin* [*s-end*]] [**dport** *d-begin* [*d-end*]] | **udp** [**sport** *s-begin* [*s-end*]] [**dport** *d-begin* [*d-end*]] | **icmp** | *protocol-num*}] [**sip-group** *sip-group-number*] [**dip-group** *dip-group-number*] [**url-group** *url-group-name* [**change-dest** *dest-ip-address*]] {**interface** *interface-name* |

	interface-group *group-name*} [**time-range** *time-rang-name*] [**track** *track-id*] [**description** *description-name*]]
Parameter Description	*app –name*: Indicates an application name. This parameter can be set to the name of the application class, application software, application software sub class, or group, or set to **any**. *priority-num*: Indicates the application routing priority, which uniquely identifies the policy. The value ranges from 1 to 10,000. *protocol-num*: Indicates ID of the IP protocol specified by APP-ROUTE. The value ranges from 1 to 255. *s-begin*: Indicates the beginning value of the source port range. The value ranges from 1 to 65535. *s-end*: Indicates the end value of the source port range. The value ranges from 1 to 65,535. It is optional and must be greater than the beginning value (***s-begin***). *d-begin*: Indicates the beginning value of the destination port range. The value ranges from 1 to 65535. *d-end*: Indicates the end value of the destination port range. The value ranges from 1 to 65535. It is optional and must be greater than the beginning value (***d-begin***). *sip-group-number*: Indicates the ID of an IP group. After the configuration, routes can be selected according to the specified source IP address. The value ranges from 1 to 1000. *dip-group-number*: Indicates the ID of an IP group. After the configuration, routes can be selected according to the specified destination IP address. The value ranges from 1 to 1000. *url-group-name*: Indicates the name of a URL group. After the configuration, routes can be selected according to the specified URL. *dest-ip-address*: Indicates the DNS server IP address in a DNS request packet matching the URL group. After the configuration, for the DNS request packet that hits the URL group, APP-ROUTE modifies the destination IP address in the packet to a specified IP address after selecting a route. *static-route*: After configuring url-group, if static route is configured with the following parameters: source IP **any**, destination IP **any**, application group **any**, a physical port, protocol **any** and a non-system group (URL group), the URLs of the URL group will be resolved automatically for a static route. *interface-name*: Indicates an interface name. *group-name*: Indicates an interface group name. *time-rang-name*: Indicates the name of the time-range object associated with a rule. *track-id*: Indicates the ID of a track. After the configuration, the status of a routing policy will be associated with the track. If the advertisement status of the track is Down, the routing policy does not take effect. Gateways of later versions do not support the URL group.
Command Mode	Global Application route policy configuration mode
Usage Guide	Use this command to configure an application route so that traffic of specified applications can be forwarded through the specified egress interface. APP-ROUTE supports applications with an identifiable initial packet of data flows. Application routing supports WAN interface and interface group. Generally, one type of applications support only one route. To configure multiple interfaces for the applications, configure an interface group. Effective time of a route can be configured through the time-range parameter. Before an application route is validated, APP-ROUTE must be enabled, the time specified by the time-range parameter is met, and at least one interface is in the UP state.

Configuring interface gateway

Command	**nexthop** *ip-address*
Parameter Description	*ip-address*: Indicates the IP address of a gateway.
Command Mode	Interface configuration mode
Usage Guide	Use this command to configure a gateway on an interface. Only non-P2P interfaces need a gateway. If an interface is selected for routing, the gateway IP address configured on the interface will be used as a next hop for forwarding packets.

Configuring Priorities of Policies

Command	**app route priority-num** *priority-number* **priority** { **increase** | **decrease** } [*1-1999*]
Parameter Description	***app –name***: Indicates an application name. This parameter can be set to the name of the application class, application software, application software sub class, or group, or set to **any**. *1-1999*: Indicates a priority interval. If the required value exceeds this value range, the parameter is automatically adjusted to the maximum value.
Command Mode	Global configuration mode
Usage Guide	Use this command to change the priorities of the application routes. The priorities of application routes are related to the configuration sequence. The application route configured later prevails over the application route configured earlier.

Configuration Example

Enabling APP-Route on Gateway

Scenario	One 50 Mbps fiber line of China Unicom and three 100 Mbps ADSLs of China Unicom are configured on the egress interface of a NetBar. All data of heavy-traffic rate-limited applications is transmitted along the ADSLs, and data of core services is transmitted along the fiber line. Rates of the video streaming media software and HTTP video applications are not limited in midnight and their traffic is transmitted along the fiber line. Traffic of China Telecom must be forwarded through the egress interface of China Telecom only.
Configuration Steps	● Configure a default route of the fiber line. FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#ip route 0.0.0.0 0.0.0.0 202.100.12.5 ● Configure an interface group that is composed of dialers 1, 2, and 3. FS (config)#interface-group intf_group FS (config-intf-group)# interface-member dialer 1 FS (config-intf-group)# interface-member dialer 2

```
FS (config-intf-group)# interface-member dialer 3
```

- Configure a DNS proxy. The fiber line of China Unicom is provided with a high priority, while the line of the dialer interface is provided with a low priority.

```
FS(config)#interface gigabitEthernet 0/5
FS(config-if-GigabitEthernet 0/5)# ip name-server 58.22.96.66 track 1
FS(config-if-GigabitEthernet 0/5)# dns-proxy priority high
FS(config)#interface dialer 1
FS(config-if-dialer 1)# ip name-server 218.85.157.99 track 2
FS(config)#interface dialer 2
FS(config-if-dialer 2)# ip name-server 218.85.157.99 track 3
FS(config)#interface dialer 3
FS(config-if-dialer 3)# ip name-server 218.85.157.99 track 4
```

- Configure an IP group and specify an address library of China Telecom.

```
FS(config)#ip-group 1
FS(config-ip-group)# route-db cnii
```

- Configure a time object.

```
FS (config)#time-range no_midnight
FS (config-time-range)#periodic daily 9:00 to 23:00
FS (config-time-range)#exit
```

- Configure APP-IDENTIFY.

```
# Configuring rate-limited application objects:
FS(config)#identify-application custom-group rate-limited traffic~route
FS(config-custom-group)#app-add P2P application software
FS(config-custom-group)#app-add software update
FS(config-custom-group)#app-add network disk
FS(config-custom-group)#app-add video|audio_MOBILE
FS(config-custom-group)#app-add download tool_MOBILE
FS(config-custom-group)#app-add HTTP download
FS(config-custom-group)#app-add HTTP upload
FS(config-custom-group)#exit
# Configuring streaming media objects:
FS(config)#identify-application custom-group streaming media~route
FS(config-custom-group)#app-add video streaming media software
FS(config-custom-group)#app-add HTTP video
```

	FS(config-custom-group)#exit ● Configure application routes. # Enabling APP-ROUTE: FS (config)#app route enable # Configuring an interface group for traffic of rate-limited applications and configuring a time period in midnight in which rates of the video streaming media software and HTTP video applications are not limited. FS (config)# app route rate-limited traffic~route interface-group intf_group time-range any FS (config)# app route streaming meida~route url-group video~sys interface intf_group time-range no_midnight FS (config)# app route any dst-grp 1 interface-group intf_group time-range any
Verification	Access an external network to check the application routing configuration and egress interface traffic information. ● Run the **show app route** command to display the application routing configuration. ● Run the **show app route statistics** command to display the general statistics about application routing. ● Run the **show app route streaming~route session** command to display the streaming media session information.

Common Errors

APP-ROUTE is not enabled.
The time-range object is not configured.
A default route is not configured.
The next hop is not configured.

3.4.2 Configuring Interface Group

Configuration Effect

Transmit traffic through a member interface according to the load policy of an interface group.

Notes

The gateway IP address must be configured on member interfaces.
Bandwidth must be configured for interfaces that use bandwidth-based load policy.

Configuration Steps

Configuring Interface Group

Mandatory.
In .global configuration mode, combine multiple interfaces to form an interface group.

Configuring Interface Members

Mandatory.

Add interfaces to the interface group.

Configuring Interface Gateway

Mandatory.

Configure the gateway function on WAN interfaces only.

Configuring Load Policy

Optional. Use this function if the load policy needs to be changed.

Use the link-based policy by default.

Configuring Interface Bandwidth

Optional. Use this function if a bandwidth negotiation error occurs or requirements cannot be met.

Negotiate about the bandwidth based on lines by default.

Verification

Check whether traffic is distributed and processed through an egress interface of the interface group.

Check the configuration of the interface group.

Related Commands

Configuring Interface Group

Command	**interface-group** *interface-group-name*
Parameter Description	*interface-group-name*: Indicates an interface group name.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure multiple egress interfaces for application routing. If the egress interfaces of an application route are specified as an interface group, traffic of data flows that hit corresponding routing policy will be distributed to the interfaces of the group.

Configuring Interface Members

Command	**interface-member** *interface-name*
Parameter Description	*interface-name*: Indicates an interface name.
Command Mode	Interface group configuration mode
Usage Guide	Use this command to add interfaces to the interface group. Only non-LAN interfaces can be added to the interface group. The virtual dialer interface is a non-LAN interface by default and can be added to the interface group.

Configuring Interface Gateway

Command	**nexthop** *ip-address*
Parameter Description	*ip-address*: Indicates the IP address of a gateway.
Command Mode	Interface configuration mode
Usage Guide	Use this command to configure a gateway on an interface. Only non-P2P interfaces need a gateway. If an interface is selected for routing, the gateway IP address configured on the interface will be used as a next hop for forwarding packets.

Configuring Load Policy

Command	**load-balance policy** { **bandwidth** | **load** }
Parameter Description	N/A
Command Mode	Interface group configuration mode
Usage Guide	APP-ROUTE balances traffic of new data flows. If a bandwidth-based policy is used, APP-ROUTE balances the traffic according to the bandwidth of different egress interfaces in a group. If a load-based policy is used, APP-ROUTE balances the traffic according to the load of different egress interfaces in a group.

Configuring Interface Bandwidth

Command	**bandwidth** *kilobits*
Parameter Description	*Kilobits*: Indicates the bandwidth of an interface (unit: kbps.)
Command Mode	Interface configuration mode
Usage Guide	Use this command to configure bandwidth of an interface. If a bandwidth-based policy is configured for an interface group, a bandwidth value needs to be configured for each interface member of the group.

Configuration Example

Creating Interface Group

Scenario	Multiple egress interfaces (GE0/1, GE0/2, and GE0/3) exist on a campus network. Egress traffic is distributed to the egress interfaces according to link load.

Configuration Steps	● Configure the interface group function in global configuration mode. FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# interface-group intf_group ● Configure interface members in interface group configuration mode. FS (config-intf-group)# interface-member GigabitEthernet 0/1 FS (config-intf-group)# interface-member GigabitEthernet 0/2 FS (config-intf-group)# interface-member GigabitEthernet 0/3 ● Enable the load-based policy function in interface group configuration mode. FS(config-intf-group)# load-balance policy load ● Configure the interface gateway in interface configuration mode. FS(config)#interface GigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# nexthop 202.101.98.54 FS(config-if-GigabitEthernet 0/1)# end FS(config)# interface GigabitEthernet 0/2 FS(config-if-GigabitEthernet 0/2)# nexthop 202.101.98.55 FS(config-if-GigabitEthernet 0/2)# end FS(config)# interface GigabitEthernet 0/3 FS(config-if-GigabitEthernet 0/3)# nexthop 202.101.98.56 FS(config-if-GigabitEthernet 0/3)# end
Verification	Check the configuration of the interface group: ● Run the **show interface-group** command to display the configuration of the interface group.

Common Errors

No interface gateway is configured.

3.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears statistical information of application routing.	**clear app route statistic**

Displaying

Description	Command

Displays the configuration information of the interface group.	**show interface-group**
Displays the application routing information.	# Displaying the configuration information of application routing. **show app route** # Displaying the statistical information of application routing. **show app route statistics** # Displaying an application object session of application routing. **show app route** *app-name* **session**

4 Configuring APP-PROXY

4.1 Overview

At present, APP-ROUTE distributes application flows depending on the initial packet identification technology. For TCP flows, due to a lack of payload in the handshake packet, the initial packet cannot be identified based on the Deep Packet Inspection (DPI) rule. APP-PROXY diverts traffic of an application to the routing link as a proxy based on the identification result to improve the application routing effect. APP-PROXY enhances the TCP flow distribution effect during application routing. Generally, it is used with APP-ROUTE in egress gateway mode.

Protocols and Standards

N/A

4.2 Applications

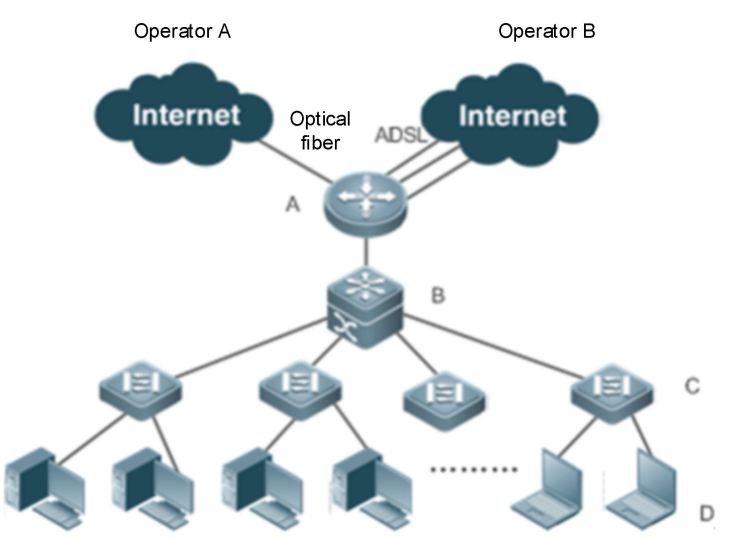
Application	Description
Deploying Egress Gateway	Deploys APP-PROXY on the egress gateway.

4.2.1 Deploying Egress Gateway

Scenario

An egress gateway can connect to lines of different operators, for example, one fiber line of China Telecom and one or multiple Asymmetric Digital Subscriber Lines (ADSLs) of China Unicom.

Figure 4- 1 Typical Application Scenario of Egress Gateway



Remarks	A indicates an egress gateway. B indicates a core switch. C indicates an access switch. D indicates an intranet PC.

Deployment

Basic NAT: Implement basic network address translation (NAT) to ensure that clients access the Internet normally.

APP-IDENTIFY: Identify the application with traffic forwarding, and cooperate with the flow control module to implement application-based flow control.

APP-ROUTE (including APP-PROXY): Enable traffic of heavy-traffic applications or key applications to be transmitted via specified egress ports based on APP-IDENTIFY.

Multilink load balancing: Distribute data flows to multiple links to ensure proper utilization of bandwidth.

Flow control: Limit the rate of P2P download flows to guarantee the traffic of key applications in combination with APP-IDENTIFY.

FLOW-AUDIT: Provide application-based flow reports in combination with APP-IDENTIFY, so that users can learn whether the egress bandwidth is sufficient and whether capacity expansion is required.

4.3 Features

Basic Concepts

↘ Data Flow

A data flow is a flow of packets with the same 5-tuple. According to protocols, data flows fall into three types: TCP flow, UDP flow, and IP flow (specific for non-TCP/UDP applications). The following table describes the 5-tuple of different data flows.

Flow Type	5-tuple Identifier
TCP flow	Source IP address|destination IP address|IP|TCP source port|TCP destination port
UDP flow	Source IP address|destination IP address|IP|UDP source port|UDP destination port
IP flow	Source IP address|destination IP address

↘ Application-based Routing

To ensure effective utilization of network resources, it is proposed that enterprises or Internet cafes rent two (or multiple) WAN links and use a line with higher quality for transmitting data of key applications that are sensitive to transmission delay and jitter and use a line with lower quality for transmitting data of P2P and other download applications. To realize the method, the egress gateway should be able to route packets based on applications. Different from the conventional IP routing technology that is based on the destination IP address of a packet, application-based routing (also referred to as application routing for short) is a routing and forwarding technology that is based on application types of data flows. With the application routing technology, data flows of different application types can be distributed to different egress ports. This separates data flows of key services from data flows of rate-limited services and minimizes impact. The major problem of application routing is how to identify the initial packet of data flows.

↘ Initial Packet Identification

The capability of identifying the first packet of each flow is initial packet identification. This function ensures the application routing effect. If packet identification starts from the midway of a data flow, the flow will be transmitted along at least two lines, which will cause flow interruption. For the TCP flow, the initial packet is a handshake packet, and the first payload packet is a request packet.

Overview

Feature	Description
APP-PROXY	Configure APP-PROXY.

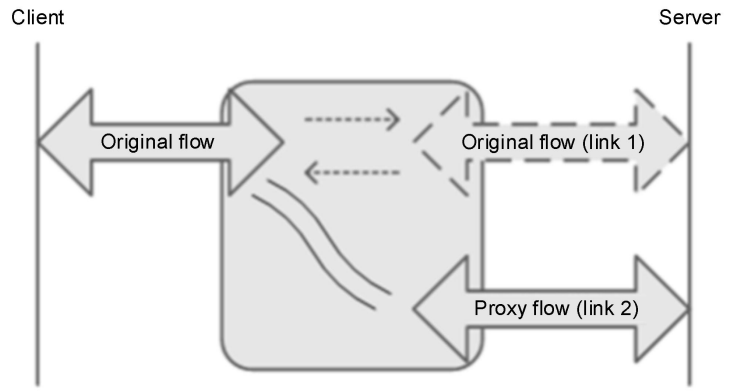
4.3.1 APP-PROXY

APP-PROXY uses the proxy technology to distribute data flows of applications, improving the traffic distribution capability during application routing.

Working Principle

APP-PROXY

After APP-PROXY identifies an application, the proxy client communicates with the server through the application routing link. This ensures that traffic is diverted to different egress ports based on the application, enhancing application routing. APP-PROXY mainly processes TCP flows, and performs refined application proxy for TCP flows with an HTTP1.1 connection. As shown in the following figure, before successful application identification, link 1 is used for data exchange with the server. Link 1 is specified for common routing. After successful application identification, link 2 is used for data exchange with the server through APP-PROXY. Link 2 is specified for application routing.



APP-PROXY works in gateway mode and does not support bridge mode. APP-PROXY does not support VPN traffic. It supports only intranet TCP flows (SYN packets and the first payload packet are initiated by the intranet).

APP-PROXY consists of HTTP APP-PROXY and TCP APP-PROXY. If a TCP flow uses an HTTP1.1 connection, it is processed by HTTP APP-PROXY. Otherwise, it is processed by TCP APP-PROXY.

APP-PROXY relies on APP-ROUTE. In terms of functions, APP-PROXY is a submodule of APP-ROUTE. If APP-ROUTE is disabled, APP-PROXY does not take effect.

Related Configuration

Enabling APP-PROXY

APP-PROXY, including HTTP APP-PROXY, is enabled by default provided that APP-IDENTIFY is enabled.

Run the app-proxy enable command to enable APP-PROXY and the no form of this command to disable APP-PROXY.

Run the app-proxy http enable command to enable HTTP APP-PROXY and the no form of this command to disable HTTP APP-PROXY.

When APP-ROUTE and APP-PROXY are enabled, and HTTP APP-PROXY is disabled, TCP APP-PROXY processes all TCP flows (including TCP flows with an HTTP1.1 connection). If TCP APP-PROXY is disabled, HTTP APP-PROXY is invalid.

4.4 Configuration

Configuration	Description and Command	
Configuring APP-PROXY	**app-proxy enable**	Enables APP-PROXY.

	app-proxy http enable	Enables HTTP APP-PROXY.

4.4.1 Configuring APP-PROXY

Configuration Effect

Configure APP-PROXY to improve the application flow distribution effect during application routing.

Notes

APP-PROXY relies on APP-IDENTIFY and APP-ROUTE. If APP-IDENTIFY or APP-ROUTE is disabled, APP-PROXY does not take effect.

APP-PROXY consists of TCP APP-PROXY and HTTP APP-PROXY. However, only APP-PROXY and HTTP APP-PROXY can be enabled or disabled.

Configuration Steps

Run the app-proxy enable command in global configuration mode to enable APP-PROXY.

Verification

Run the show app-proxy enable command to display the APP-PROXY status.

Related Commands

- Enabling APP-PROXY

Command	app-proxy enable
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

- Enabling HTTP APP-PROXY

Command	app-proxy http enable
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

- Displaying APP-PROXY Status

Command	show app-proxy enable
Parameter Description	N/A
Command	Privileged EXEC mode, global configuration mode, or interface configuration mode

Mode	
Usage Guide	N/A

Configuration Example

Enabling APP-PROXY

Configuration Steps	Enable APP-PROXY. Enable HTTP APP-PROXY.
	FS# configure terminal FS(config)#app-proxy enable FS(config)#app-proxy http enable
Verification	Display the APP-PROXY status.
	FS#show app-proxy enable app-proxy : Y app-proxy http : Y

Common Errors

APP-PROXY does not take affect even if it is enabled when APP-ROUTE is configured but not enabled.

4.5 Monitoring

Displaying

Description	Command
Displays APP-PROXY information.	**show app-proxy enable**

5 Configuring User Session Limit

5.1 Overview

The rapid development of Internet technology makes categories and quantities of application on WAN continuously increase, such as on-line game, video session, voice over internet protocol (VOIP), E-mail, P2P application and so on. Since P2P demands a large amount of streaming sessions resources and bandwidth resources, it made the bandwidth of enterprise, Internet bar and college became in great demand which is abundant previously, and meanwhile, it also put forward higher requirements for the gateways. Global session limit is mainly used in the following scenarios:

How to efficiently allocate the limited output link bandwidth and thus to avoid slow-speed network result from individual download. Except QOS or other flow control, global session limit can also achieve the purpose of controlling output link bandwidth to a certain extent.

How to efficiently allocate the limited gateway/bridge device session resources (as each conversation will consume certain internal storage of gateway /bridge, while the gateway/bridge resource is limited, so the session resource is also limited). In the following scenarios, we can achieve the goal through global session limit.

Avoid gateway/bridge device resources being consumed up by large session resource consumption by individual P2P downloading.

Avoid consuming too much session resources due to the infected internal PC which may launch a plenty of sessions.

Avoid wasting session resources due to establishing meaningless sessions by the device.

5.2 Applications

Application	Description
Establishing Internal Network Session Number	Typical enterprise environment, where each IP address is set with a certain limit of the sessions

5.2.1 Establishing Internal Network Session Number

Scenario

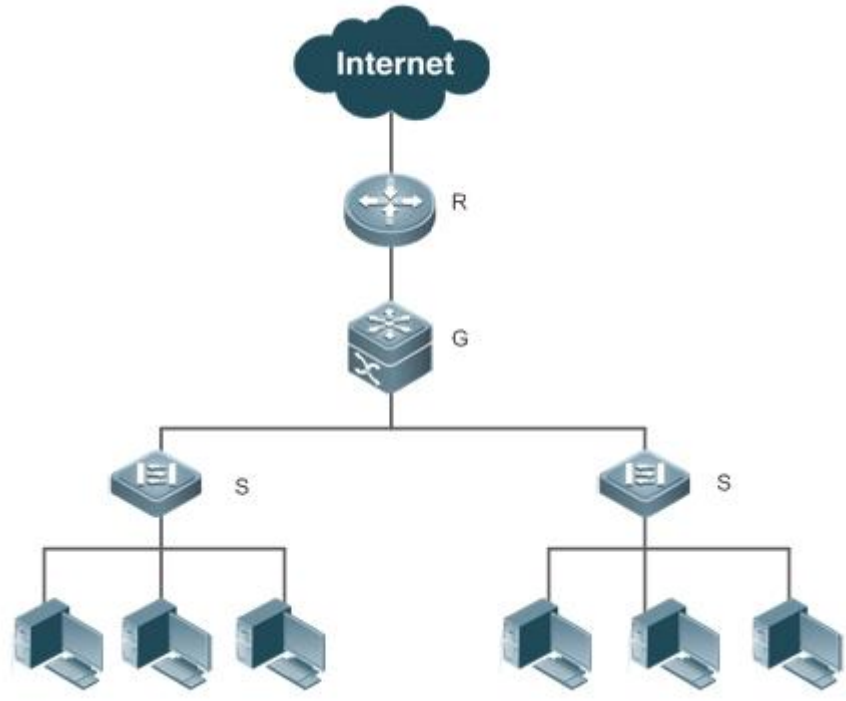
In a typical enterprise environment, it is used to achieve the following functions:

Set allowed streaming session number to less than 200,000;

Set allowed streaming session number of each IP address to less than 500;

Set allowed streaming session number of each management IP address to less than 1,000;

Figure 5- 1



Remarks	R is an output gateway device. G is a core switch. S is an access equipment.

Deployment

Configure the leader subscriber group and the subscriber information.

Set the default global IP session limit.

Set session limit for the leaders separately.

5.3 Features

Basic Concepts

↘ Session

The flows with the same value of 5-tuple (internal IP address, inside interface, external IP address, outside interface and protocol) are belong to one session. Normally, FS gateway products will allocate session resources for each normal communication session to guarantee normal communicating sessions.

Feature

Overview	Description
Global Session Limit Switch	Quickly enables or disables global session number.
Global Session Total Limit	Sets limit to the session number allowed for the entire system device.
Session Limit Based on Subscriber/Subscriber-group	Configures session limit based on subscriber/subscriber-group, for instance setting 300 sessions for User A and 500 sessions for User B.

Configuring ACL-based Session Limit	Configures session limit based on ACL and restrain the session reaching the limit based on specified ACL.
Uplink Packet Rate Limit	Limits the rate of uplink packets from the intranet.
New Session Protection on Device	Prevents new session capacity insufficiency from affecting network experience.

5.3.1 Global Session Limit Switch

Use this function switch to close global session limit without eliminating the existing global session limit rule.

Working Principle

Before setting limit to global session number, the judgment on whether the switch is closed shall be made. If it was closed, then no limit will be set to the session number.

Related Configuration

Configuring Global Session Limit Switch

The global session number switch is on by default. Configured with the limit, the global session limit will be enabled.
You can use the no flow-pre-mgr enable command to close global session limit switch and use the flow-pre-mgr enable command to open global session limit.

5.3.2 Global Session Total Limit

Every session will consume some certain resources of the device in normal condition. While in certain condition, the session limit is set for an entire device system to control such resource consumption within a specific range.

Working Principle

When requesting resource for a session, the device will judge whether the session number reaches the limit. If the session limit is already reached, the new session will not be created.

Related Configuration

Configuring the Total Limit Number of Session

The session number allowed by the device depends on system resource (flow table capacity) by default.
You can use the flow-pre-mgr total-limit command to configure the limit. Normally this parameter needn't be set.

5.3.3 Session Limit Based on Subscriber/Subscriber-group

Configure session limit based on subscriber/subscriber-group, for instance setting 300 sessions for User A and 500 sessions for User B.

Working Principle

Session limit based on subscriber/subscriber-group depends on subscriber identification. When the subscriber/subscriber-group information of a session is identified, we need to judge whether the session number of the subscriber/subscriber-group reaches the limit. If the limit is already reached, the new session of the subscriber/subscriber-group will not be created. Otherwise, a new session will be created as normal.

Related Configuration

Configuring the Session Limit Based on Subscriber/Subscriber Group

Use the flow-pre-mgr rule-id subscriber subs_name action { block | by-pass | { trust total-limit total-limit-number per-ip-limit per-limit-number } } command to set session limit to subscriber/subscriber-group. Normally, it is recommended to set session limit for every IP address from 500 to 1,000.

5.4 User/User Group-based UDP Session Limit

Based on a user/user group, set the limit ratio of UDP sessions of per user to total sessions. For example, set the limit value of the sessions per user to 3000 for User A/User Group A and set the percentage of UDP sessions to 50%. Then, the UDP streaming sessions of this user/user group cannot exceed 1500 (that is, 3000 * 50%).

Working Principle

The user/user group-based UDP session limit relies on the per-IP-based streaming session limit rule with the user/user group-based streaming session control mode of trust. When information about a user/user group of a session is identified, the system checks whether the number of UDP sessions of the user/user group exceeds the limit. If yes, the system will not permit the session. If not, the system creates a UDP session.

Related Configuration

Setting the User/User Group-based Session Limit

By default, the limit ratio of UDP sessions to total sessions is 0, indicating no limitation.

Run the **flow-pre-mgr per-ip-limit udp-ratio** *ratio* command to set the limit ratio of user/user group-based UDP sessions to total sessions. It is recommended to set the ratio to 50%.

5.4.1 ACL-based Session Limit

Configure session limit based on ACL and restrain the session reaching the limit based on ACL from creating.

Working Principle

A judgment shall be made about whether the session coincident with specified ACL reached the limit or not. If it reached the limit, no more such session will be created. Otherwise, a new session will be created as normal.

Related Configuration

Configuring the ACL-based Session Limit

Use the flow-pre-mgr rule-id access-list acl-number action { block | by-pass | { trust total-limit total-limit-number } } command to configure the ACL-based session limit. ACL-based session limit cannot configure the session limit per IP address. Normally, this feature is to set limit to sessions for some kinds (like attack) to avoid too much resource consumption.

5.4.2 Per IP Address Uplink PPS Limit Based on IP

Set limit to per IP address uplink PPS based on IP, for example setting a maximum of 5,000 uplink packets per second per IP address. It is often used to defend against the uplink traffic attack.

Working Principle

Per IP address uplink PPS limit is set based on IP address. When the uplink rate surpasses the limit, the excessive packets will be dropped.

Related Configuration

Configuring Uplink Packet Rate Limit for IP Address

No uplink packet rate limit is configured by default.

Run the flow-pre-mgr upload-pps-limit limit-number command to configure the uplink packet rate limit for a real IP address.

Run the flow-pre-mgr upload-pps-limit virtual-host limit limit-number command to configure the uplink packet rate limit for a virtual IP address.

Run the flow-pre-mgr upload-pps-limit { specify ip-addr | specify-range ip-start ip-end | specify-subnet ip-subnet ip-mask } limit limit-number command to configure the limit value for a single IP address, IP range, and IP segment.

5.4.3 New Session Protection on Device

New packets are filtered based on the ACL to block unnecessary new sessions. Limit based on IP address is set for per IP address new session speed. IP address can be divided into virtual IP address (constructed IP address) and real IP address. All IP addresses labeled as virtual IP address use one new session rate limit and all real IP addresses have their own respective new session rate limit. It is often used to defend against the new attack from internal network.

Working Principle

The new session rate is controlled, and when the new session rate exceeds the limit, new packets are discarded.

Related Configuration

Configuring New Session Rate Limit Per IP Address

No rate limit is configured by default.

Run the ip session filter acl-id command to filter flows allowed by the device.

Run the flow-pre-mgr protocol-enable command to allow the OSPF,VRRP, and RIP protocols.

Run the following command to allow or block uplink new sessions: flow-pre-mgr { up-deny | up-permit } id { { { ip | icmp | ospf } { src-host ip-addr | src-range ip-start ip-end | src-subnet ip-subnet ip-mask } { dst-host { ip-addr | any } | dst-range { ip-start ip-end | any } | dst-subnet { ip-subnet ip-mask | any } } } | { { tcp | udp } { src-host ip-addr | src-range ip-start ip-end | src-subnet ip-subnet ip-mask } { src-port { port | any } | sport-range { port-srart port-end | any } } { dst-host {ip-addr | any} | dst-range { ip-start ip-end | any } | dst-subnet { ip-subnet ip-mask | any } } { dst-port { port | any } | dport-range { port-srart port-end | any } } } }.

Run the following command to allow or block downlink new sessions: flow-pre-mgr { down -deny | down -permit } id { { { ip | icmp | ospf } { src-host { ip-addr | any } | src-range { ip-start ip-end | any } | src-subnet { ip-subnet ip-mask | any } } { dst-host ip-addr | dst-range ip-start ip-end | dst-subnet ip-subnet ip-mask } } | { { tcp | udp } { src-host { ip-addr | any } | src-range { ip-start ip-end | any } | src-subnet { ip-subnet ip-mask | any } } { src-port { port | any } | sport-range { port-srart port-end | any } } { dst-host ip-addr | dst-range ip-start ip-end | dst-subnet ip-subnet ip-mask } { dst-port { port | any } | dport-range { port-srart port-end | any } } } }.

Run the flow-pre-mgr new-session-limit { start-up | virtual-host | real-host } limit limit-number command to configure the new session rate limit for virtual and real IP addresses within three minutes after the startup.

Run the flow-pre-mgr new-session-limit { specify ip-addr | specify-range ip-start ip-end | specify-subnet ip-subnet ip-mask } limit limit-number command to configure the new session rate limit for a specific IP address, IP range, and IP segment.

5.5 Configuration

Configuration	Description and Command	
Enabling Global Session Limit.	(Mandatory) It is used to enable global session limit. IP address uplink PPS and new session limit are configured according to the actual network conditions.	
	flow-pre-mgr enable	Enables global session limit.
	flow-pre-mgr total-limit	Configures the total-limit-number of session.
	flow-pre-mgr subscriber	Configures the session limit based on subscriber/subscriber group.
	flow-pre-mgr access-list	Configures ACL-based session limit.
	flow-pre-mgr priority-swap	Changes the priority levels of two rules.
	flow-pre-mgr protocol-enable	Allows a protocol.
	flow-pre-mgr upload-pps-limit	Configures the uplink packet rate limit of a real IP address.
	flow-pre-mgr upload-pps-limit virtual-host limit	Configures the uplink packet rate limit of a virtual IP address.
	flow-pre-mgr upload-pps-limit specify	Specifies the uplink packet rate limit of the real host at a specific IP address.
	flow-pre-mgr upload-pps-limit specify-range	Specifies the uplink packet rate limit of the real host in a specific IP range.
	flow-pre-mgr upload-pps-limit specify-subnet	Specifies the uplink packet rate limit of the real host in a specific IP segment.
	flow-pre-mgr new-session-limit start-up	Configures the new session limit of all virtual IP addresses within 3 minutes after the start up.
	flow-pre-mgr new-session-limit virtual-host	Configures the new session limit of all virtual IP addresses when the device is in normal operation.
	flow-pre-mgr new-session-limit real-host	Configures new session rate limit for real IP address.
	flow-pre-mgr new-session-limit specify	Configures new session limit to the real host of the specified IP address.
	flow-pre-mgr new-session-limit specify-range	Configures the new session limit for the real host in a specified IP range.
	flow-pre-mgr new-session-limit specify-subnet	Configures the new session limit for the real host of a specified IP segment.

	Ip session filter	Configures the device to filter new packets.
	flow-pre-mgr up-deny	Blocks uplink new flows.
	flow-pre-mgr up-permit	Allows uplink new flows.
	flow-pre-mgr down-deny	Blocks downlink new flows.
	flow-pre-mgr down-permit	Allows new downlink flows.

5.5.1 Configuring Global Session Limit

Configuration Effect

Enable total session limit of the device.
Enable the session limit based on subscriber/subscriber group.
Enable the session limit based on ACL.

Notes

When configuring session limit based subscriber/subscriber group, you need first enable the Layer23 Classification and configure the subscriber/subscriber group information.
Rules configured by the system follow the principle that the later configured rule will be prior, i.e. the latest configured rule has the highest priority level.

Configuration Steps

Enabling/Disabling Global Session Limit

Optional. It is enabled by default. If you want to disable the function without delete the rule of global session limit, you can achieve it by making the switch in the OFF state.
The function shall be disabled on the gateways that do not need it and STAs need this feature do not have to be configured.

Configuring Total Session Limit

Optional.
If limit is set to the total session, then this feature must be configured.
Limit is set to each of the gateways requiring total session limit. Except otherwise required, this feature needn't be configured.

Configuring the Session Limit Based on Subscriber/Subscriber Group

Optional.
If session limit based on subscriber/subscriber-group is required, then this feature must be configured.
Every gateway need session limit based on subscriber/subscriber-group shall has the following configuration: first enabling layer23 subscriber identification and configuring specific subscriber/subscriber-group information, then configuring session limit for the specified subscriber/subscriber-group. Normally, it is recommended to set the limit to 500 to 1,000 for every IP address.

Configuring ACL-based Session Limit

Optional.
If session limit based on ACL is required, then this feature must be configured.
Every gateway need session limit based on ACL shall has the following configuration: configuring session limit for the specified ACL. ACL-based session limit feature cannot configure per IP address session limit. Normally, this feature is to set with limit to sessions of some

kinds (like attack) to avoids too much resource consumption.

Changing the Priority Levels of Two Rules

Optional.

This configuration must be used when you want to switch the priority level of two rules of a STA.

The configuration of rules follows the principle that the later configured rule will be preferentially valid. The priority level switch of two rules can be made by using this configuration.

Configuring Uplink Packets Rate Limit for Intranet IP Address

Optional.

It is recommended to enable this function when defending against uplink traffic attack.

Configuring Internal IP Address New Session Limit

Optional.

It is recommended to enable this function when defending against new session attack.

Configuring Filtering Condition for New Flows

Optical.

Enable this function when there is a large number of unnecessary flows (for example, attack flows).

Verification

When there is numerous sessions, check the following information:

Configuration and matching information of every rule;

Session and session limit of each IP address.

Whether there are attack logs.

Related Commands

Enabling/Disabling Global Session Limit

Command	**flow-pre-mgr enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	You can use this command to enable global session limit, which is enabled by default. You can use the **no** form of the **no flow-pre-mgr enable** command to disable global session number.

Configuring Total Session Limit

Command	**flow-pre-mgr total-limit** *limit-number*
Parameter Description	Limit-number: the global streaming limit, whose range depends on the device memory, where 0 represents that there is no limit.
Command	Global configuration mode

Mode	
Usage Guide	1) You can use the **no** form of the **flow-pre-mgr id** command in global configuration mode to delete the relative configuration. 2) The RAM of the device decides the maximum number of the supported streaming session. When configuring this command, you are able to input the maximum number of streaming session that the device supports. 3) In gateway mode, we recommend not to set restriction on sticky-load-balancing data flow, which results from the bad performance of the router at superior hierarchical level.

Configuring Subscriber-based Session Limit

Command	**flow-pre-mgr** *rule-id* **subscriber** *subs_name* **action** { **block** | **by-pass** | { **trust total-limit** *total-limit-number* **per-ip-limit** *per-limit-number* } }
Parameter Description	*rule-id:* rule identifier ranging from 1 to 50. When the configured identifier was obsessed, the configuration will fail, prompted with collision message; *subs_name*: rule-associated static subscriber or static subscriber group; *total-limit-number*: total limit number of the streaming session based on subscriber/subscriber group, whose range depends on the device memory, where 0 represents that there is no limit. *Per-limit-number*: The per IP address streaming session limit of subscriber/subscriber group, whose range depends on the device memory but not larger than total-limit-number, where 0 represents that there is no limit.
Command Mode	Global configuration mode
Usage Guide	1) You can use the following control mode of the streaming session based on subscriber/subscriber group: block, by-pass or trust. If want to delete the relative configuration, you can use the **no** form of the **flow-pre-mgr id** command. 2) Configured rules have their priorities, which will follow the latest configured rule with the highest priority level. 3) About the actions, block means that no streaming session communication is allowed, by-pass means that packets can be forwarded according to the bridge mapping relationship without creating streaming session (this keyword only appears in bridging mode and single-arm mode but not gateway made); trust means that you can configure the total-limit- number and per-limit-number of the streaming session based on subscriber/subscriber group, and streaming session will not continue when the number of streaming session reaches the limit. 4) The RAM of the device decides the maximum number of the supported streaming session. When configuring this command, you are able to input the maximum number of streaming session that the device supports. 5) In gateway mode, we recommend not to set restriction on sticky-load-balancing data flow, which results from the bad performance of the router at superior hierarchical level.

Configuring the ACL-based Session Number

Command	**flow-pre-mgr** *rule-id* **access-list** *acl-number* **action** { **block** | **by-pass** | { **trust total-limit** *total-limit-number* } }
Parameter Description	*rule-id:* rule identifier ranging from 1 to 50. When the configured identifier was obsessed, the configuration will fail, prompted with collision message; *acl-number*: rule-associated ACL number, ranging from 1 to 199.

	total-limit-number: total limit number of ACL streaming session, whose range depends on the device memory, where 0 represents that there is no limit.
Command Mode	Global configuration mode
Usage Guide	1) You can use the following control mode of the ACL-based streaming session: block, by-pass or trust. If want to delete the relative configuration, you can use the **no** form of the **flow-pre-mgr id** command. 2) Configured rules have their priorities, which will follow the latest configured rule with the highest priority level. 3) You cannot configure any streaming session limit per IP address based on ACL. 4) About the actions, block means that no streaming session communication is allowed, by-pass means that packets can be forwarded according to the bridge mapping relationship without creating streaming session (this keyword only appears in bridging mode and single-arm mode but not gateway made); trust means that you can configure the total limit of the ACL-based streaming session, and streaming session will continue when the number of streaming session reaches the limit. 5)The source IP address of the ACL corresponds with the internal network IP address, the source interface with the internal interface, the destination IP address with the external network IP address, and the destination interface with the external network interface. 6) The RAM of the device decides the maximum number of the supported streaming session. When configuring this command, you are able to input the maximum number of streaming session that the device supports. 7) It is recommended not to configure too many sessions, as the limit rule of streaming session affects the performance of the device greatly. This rule is often used to avoid creating pointless streaming sessions. Please find the examples below. 8) The rule-associated ACL entry only allows the configuration of source IP address, source interface, destination IP address, destination interface and protocol number, otherwise this ACL entry will be invalid in this module. 9) In gateway mode, we recommend not to set restriction on sticky-load-balancing data flow, which is resulted by the bad performance of the router at superior hierarchical level.

Changing the Priority Levels of Two Rules

Command	**flow-pre-mgr priority-swap** *rule-id1 rule-id2*
Parameter Description	The *rule-id1* and *rule-id2* are the IDs of two rules to be switched.
Command Mode	Global configuration mode
Usage Guide	Both Rule-id 1 and Rule-id 2 must exist, otherwise the command is invalid. If Rule-id 1 is same as Rule-id 2, this command will change nothing.

Configuring Per IP Address Uplink PPS Limit

Command	**flow-pre-mgr upload-pps-limit** *limit-number*
Parameter Description	*limit-number;* limit of uplink packet speed, ranging from 0 to 100,000

Command Mode	Global configuration mode
Usage Guide	All real IP addresses have a same uplink rate limit, but the respective uplink rate is calculated based on each IP address. A proper rate limit needs to be configured; otherwise, a network abnormality may occur. It is recommend to set the value between **3000** and **5000**. The value **0** means no limit. Run the **specify** command to configure the rate limit for servers and the like.

Configuring Uplink PPS Limit for Specified IP Addresses

Command	**flow-pre-mgr upload-pps-limit** { **specify** *ip-addr* | **specify-range** *ip-start ip-end* | **specify-subnet** *ip-subnet ip-mask* } **limit** *limit-number*
Parameter Description	*ip-addr:* Indicates a specified IP address. *ip-start:* Indicates the start IP address in a specified IP range. *ip-end:* Indicates the end IP address in a specified IP range. *ip-subnet:* Specifies a subnet segment. *ip-mask:* Specifies a mask. *limit-number:* Indicates the uplink packet rate limit. The value range is from **0** to **100,000**.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure the rate limit for special IP addresses (such as IP addresses of servers) to which the real-host parameter is not applicable. The rate limit value must be appropriate. An excessively large value may cause protection failures while an excessively small value may cause abnormal access to these IP addresses. It is recommended to set the value between 10,000 and 20,000 based on the network environment. If a real IP address is identified as a virtual IP address, run this command to add the IP address to real IP addresses.

Filtering New Packets and Blocking Invalid New Session

Command	**ip session filter** *acl-id*
Parameter Description	*acl-id:* Indicates the ACL ID.
Command Mode	Global configuration mode
Usage Guide	The principle of new packet filtering is to allow valid packets and block invalid packets in the network environment. Valid packets are packets send from real IP addresses in the network environment. Invalid packets are packets send from IP addresses that do not exist in the network environment, such as IP addresses forged in D/DOS attacks.

Filtering Uplink New Packets and Blocking Invalid New Session

Command	**flow-pre-mgr** { **up-deny** | **up-permit** } *id* { { { ip | icmp | ospf } { **src-host** *ip-addr* | **src-range** *ip-start ip-end* | **src-subnet** *ip-subnet ip-mask* } { **dst-host** { *ip-addr* | **any** } | **dst-range** { *ip-start ip-end* | **any** } | **dst-subnet** { *ip-subnet ip-mask* | **any** } } } | { { tcp | udp } { **src-host** *ip-addr* | **src-range** *ip-start ip-end* | **src-subnet** *ip-subnet ip-mask* } { **src-port** { *port* |

	any } | **sport-range** { *port-srart port-end* | **any** } } { **dst-host** {*ip-addr* | **any**} | **dst-range** { *ip-start ip-end* | **any** } | **dst-subnet** { *ip-subnet ip-mask* | **any** } } { **dst-port** { *port* | **any** } | **dport-range** { *port-srart port-end* | **any** } } } }
Parameter Description	*ip-addr:* Indicates a specified IP address. *ip-start:* Indicates the start IP address in a specified IP range. *ip-end:* Indicates the end IP address in a specified IP range. *ip-subnet:* Specifies a subnet segment. *ip-mask:* Specifies a mask. *port:* Indicates a port. *port-srart:* Indicates the start port in a port range. *port-end:* Indicates the end port in a port range.
Command Mode	Global configuration mode
Usage Guide	The principle of new packet filtering is to allow valid packets and block invalid packets in the network environment. Valid packets are packets send from real IP addresses in the network environment. Invalid packets are packets send from IP addresses that do not exist in the network environment, such as IP addresses forged in D/DOS attacks. Both this command and the **ip session filter** command are used to filter uplink packets. This command is used because filtering performance of the **ip session filter** command is poor. This command is used together with the downlink new packet filtering command when there is a large number of ACEs. The source IP address cannot be set to **any** when this command is configured.

Filtering Downlink New Packets and Blocking Invalid New Session

Command	**flow-pre-mgr** { **down -deny** | **down -permit** } *id* { { { ip | icmp | ospf } { **src-host** { *ip-addr* | **any** } | **src-range** { *ip-start ip-end* | **any** } | **src-subnet** { *ip-subnet ip-mask* /**any** } } { **dst-host** *ip-addr* | **dst-range** *ip-start ip-end* | **dst-subnet** *ip-subnet ip-mask* } } | { { tcp | udp } { **src-host** { *ip-addr* | **any** } | **src-range** { *ip-start ip-end* | **any** } | **src-subnet** { *ip-subnet ip-mask* /**any** } } { **src-port** { *port* | **any** } | **sport-range** { *port-srart port-end* | **any** } } { **dst-host** *ip-addr* | **dst-range** *ip-start ip-end* | **dst-subnet** *ip-subnet ip-mask* } { **dst-port** { *port* | **any** } | **dport-range** { *port-srart port-end* | **any** } } } }
Parameter Description	*ip-addr:* Indicates a specified IP address. *ip-start:* Indicates the start IP address in a specified IP range. *ip-end:* Indicates the end IP address in a specified IP range. *ip-subnet:* Specifies a subnet segment. *ip-mask:* Specifies a mask. *port:* Indicates a port. *port-srart:* Indicates the start port in a port range. *port-end:* Indicates the end port in a port range.
Command Mode	Global configuration mode
Usage Guide	The principle of new packet filtering is to allow valid packets and block invalid packets in the network environment. Valid packets are packets send from real IP addresses in the network environment.

	Invalid packets are packets send from IP addresses that do not exist in the network environment, such as IP addresses forged in D/DOS attacks. Both this command and the **ip session filter** command are used to filter downlink packets. This command is used because filtering performance of the **ip session filter** command is poor. This command is used together with the uplink new packet filtering command when there is a large number of ACEs. The destination IP address cannot be set to **any** when this command is configured.

Allowing OSPF, VRRP, and RIP Protocols

Command	**flow-pre-mgr protocol-enable**
Parameter Description	*N/A*
Command Mode	Global configuration mode
Usage Guide	Allow the OSPF, VRRP, and RIP protocols to be free from the new session rate limit and from the concurrent session limit.

Configuring New Session Limit

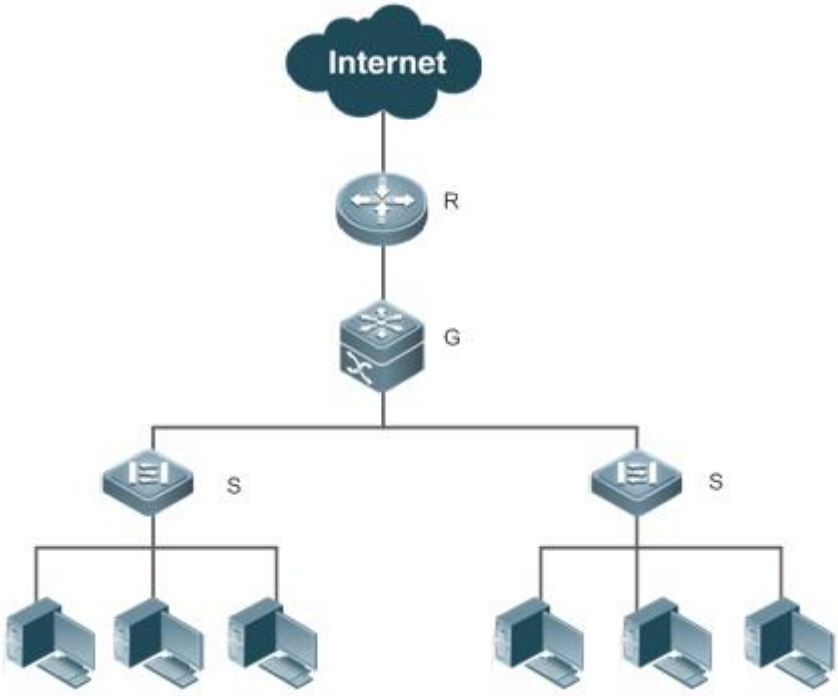
Command	**flow-pre-mgr new-session-limit** { **start-up** | **virtual-host** | **real-host** } **limit** *limit-number*
Parameter Description	*limit-number:* Indicates the range of the new session limit for an IP address, which is from **0** to **100,000**.
Command Mode	Global configuration mode
Usage Guide	start-up: Indicates the new session limit during startup. Users at intranet IP addresses go online in a centralized manner during device startup. Each IP address is considered as a virtual IP address before a TCP flow is created from this IP address. The new session limit is accumulated based on all IP addresses. If this parameter is set to an excessively small value, go-online of users at the intranet IP addresses is affected. Therefore, this parameter can be set to a relatively large value (20,000 to 30,000). Virtual-host: Indicates a virtual IP address. During normal running of the device, TCP connections are created at all normal intranet IP addresses, and the intranet IP addresses no longer belong to virtual IP addresses. If an IP address is still identified as a virtual IP address, the IP address is possibly an attack source. Therefore, when the device runs normally, the new session rate for virtual IP addresses can be set to a value slightly less than that for new session within three minutes after the startup. Because newly online IP addresses without TCP connections created are also considered as virtual IP addresses, if the rate limit is set to an excessively small value, user go-online is affected once the capacity is used up by attacks. Therefore, it is recommended to set the rate limit to an appropriate value, for example, the empirical value **3000**. Real-host: Indicates a real IP address. After an intranet IP address has a TCP connection created, the device identifies the IP address as a real IP address. In this case, the default new session limit is used. This command is used to configure the default new session limit for real IP addresses.

Configuring New Session Limit to the Real Host of the Specified IP Address

Command	**flow-pre-mgr new-session-limit** { **specify** *ip-addr* | **specify-range** *ip-start ip-end* | **specify-subnet** *ip-subnet ip-mask* } **limit** *limit-number*
Parameter Description	*ip-addr:* Indicates a specified IP address. *ip-start:* Indicates the start IP address in a specified IP range. *ip-end:* Indicates the end IP address in a specified IP range. *ip-subnet:* Specifies a subnet segment. *ip-mask:* Specifies a mask. *limit-number:* Indicates the uplink packet rate limit. The value range is from **0** to **100,000**.
Command Mode	Global configuration mode
Usage Guide	You can use this command to configure new session limit for all real IP addresses, where some special real IP addresses, like those of servers, shall be configured otherwise. Besides that, if a real IP address is identified as virtual, you can use this command to label it as a real one.

Configuration Examples

Configuring Global Session Number in Typical Enterprise Environment

Scenario **Figure 5–2**	
Configuration Steps	● Set allowed streaming session number to less than 200,000; ● Set allowed streaming session number of each IP address to less than 500; ● Set allowed streaming session number of each management IP address to less than 1000; ● Set the new session rate limit for common clients in the company to **300**. ● Set the new session rate for the server network segment (192.168.4.0/24) of company to **1000**.

R	1) Configuring subscriber information #Enter global configuration. R# configure terminal Enter configuration commands, one per line. End with CNTL/Z. #Configure leader subscriber group. R(config)# subscriber static name LeaderGroup parent / #Configure leader subscriber information. R(config)# subscriber static name LeaderA parent /LeaderGroup ip-host 192.168.5.11 R(config)# subscriber static name LeaderB parent /LeaderGroup ip-host 192.168.5.12 2) Configuring rules of pre-creation limit and management for streaming session number. #Configure global session limit R(config)# flow-pre-mgr total-limit 200000 #Configure streaming session limit for all subscribers R(config)# flow-pre-mgr subscriber any action trust total-limit 0 per-ip-limit 500 #Configure streaming session limit for leader subscriber group. R(config)# flow-pre-mgr subscriber LeaderGroup action trust total-limit 0 per-ip-limit 1000 3) Configuring new session rate limit for common clients #Configure the new session rate used within 3 minutes after startup. R(config)# flow-pre-mgr new-session-limit start-up limit 20000 #Configure the new session rate limit for virtual IP addresses. R(config)# flow-pre-mgr new-session-limit virtual-host limit 3000 #Configure the new session rate limit for common clients. R(config)# flow-pre-mgr new-session-limit real-host limit 300 4) Configuring the new session rate limit for servers #Configure the new session rate for a specified network segment. R(config)# flow-pre-mgr new-session-limit specify-subnet 192.168.4.0 255.255.255.0 limit 1000
Verification	When there is numerous sessions, check the following information: ● the configuration and matching information of every rule; ● the session and session limit of each IP address.
	R# show flow-pre-mgr rule-info R# show flow-pre-mgr ip-info R# show flow-pre-mgr new-session-limit attack R# show flow-pre-mgr drop-count

Common Errors

Before configuring subscriber/subscriber group session limit feature, the relevant subscriber/subscriber group information is not configured and Layer23 Classification is not enabled.

The rule of ACL-based session limit is configured while the relevant ACL is not.

ACL-based session limit supports only the ACL of 5-tuple flow (internal IP address, inside interface, external IP address, outside interface and protocol). In case it is configured otherwise, it will actually be invalid.

5.6 Monitoring

Displaying

Description	Command
Displays configured rules.	**show flow-pre-mgr rule-info**
Displays the session number and limit of an IP address.	**show flow-pre-mgr ip-info** [*ip-address*]
Displays the configuration parameter for defense against uplink traffic attack.	**show flow-pre-mgr upload-pps-limit**
Displays the configuration parameter for defense against new session attack.	**show flow-pre-mgr new-session-limit**
Displays the log of the latest new session attack.	**show flow-pre-mgr new-session-limit attack**
Displays packet loss caused by attack defense.	**show flow-pre-mgr drop-count**

6 Configuring Flow Control

6.1 Overview

Flow control is a mechanism that classifies flows according to some rules to implement differentiated forwarding and packet loss.

The flow control solution can be carried out to guarantee the critical flow and suppress the malicious flow.

Flow control can be enabled when the bandwidth is insufficient and the flow needs to be distributed reasonably.

6.2 Applications

Flow control adopts the following methods to classify flows:

Classification based on Layer 2 (VID)

Classification based on user, where the user classification object contains the mapping relationship between user name and intranet source IP address

Classification based on network

Classification based on authentication object; all the authentication objects are matched by default

Classification based on application identification, supporting user-defined protocol classification objects

Classification based on VPN packet

Classification based on time segment

Classification based on account

More than one of the above classifications can be used together. For example, the network classification and application classification can be specified at the same time. Therefore, many combinations of classifications can implement different scenarios. The table below lists the typical application scenarios of flow control:

Applications	Description
Flow Control Based on Application_Providing multicast service in an AS	Applications are differentiated by priority, and those with a higher priority will be first guaranteed. For example, games are given priority over videos.
Flow Control Based on IP Address	Users are differentiated by priority, and those with a higher priority will be first guaranteed. For example, VIP customers are given priority over common customers.
Flow Control Based on Time Segment	Flows are classified by time segment and treated differently. For example, network access can be disabled in working hours.
Flow Control Based on Account	The bandwidth is distributed based on account. For example, the bandwidth of a student account is restricted to 4 Mbps, regardless of the number of terminals.

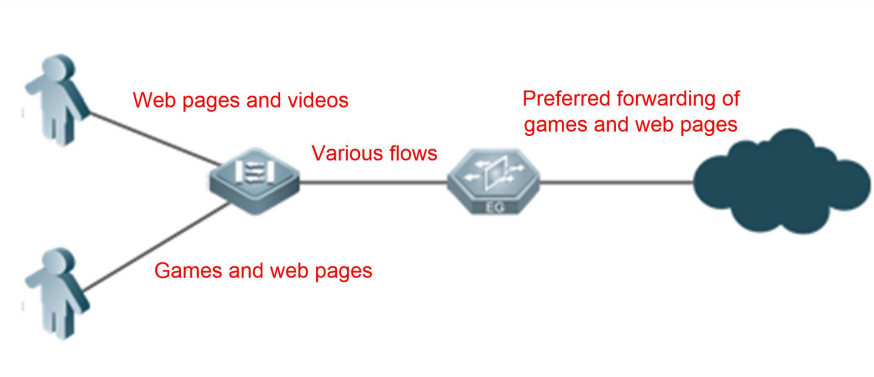
6.2.1 Flow Control Based on Application

Scenario

In some environments, the user wishes to prioritize applications and first guarantee the applications with high priority.

Take the Internet café as an example, games and Internet access have the highest priority, and videos are at the lowest priority. In this case, flow control based on application can be configured to first guarantee key applications such as games and Internet access, as shown in the following figure.

Figure 6-1



Deployment

Configure a flow control channel.

Configure a flow control policy.

Enable the application identification function.

6.2.2 Flow Control Based on IP Address

Scenario

In some environments, the user wishes to prioritize users and first guarantee VIP customers.

Flow control based on IP address can be configured in this scenario. For example, the user has two types of customers: students and teachers; the user wishes to allocate 10 Mbps bandwidth to teachers and 2 Mbps bandwidth to students, as shown in the following figure.

Figure 6-2

Deployment

Configure a flow control channel.

Configure a flow control policy.

Enable the user identification function.

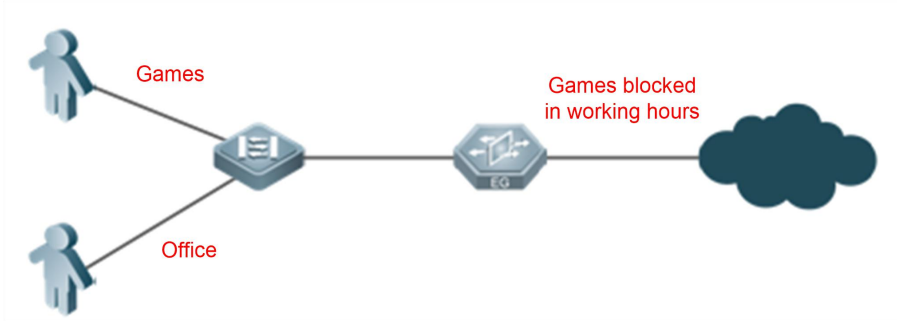
6.2.3 Flow Control Based on Time Segment

Scenario

In some scenarios, the user needs to set different flow control solutions in different time segments. In this case, flow control based on time segment can be configured. For example, a company can prevent employees from playing games in working hours, as shown in the

following figure.

Figure 6-3



Deployment

Configure a flow control channel.

Configure a flow control policy.

Configure a time segment object.

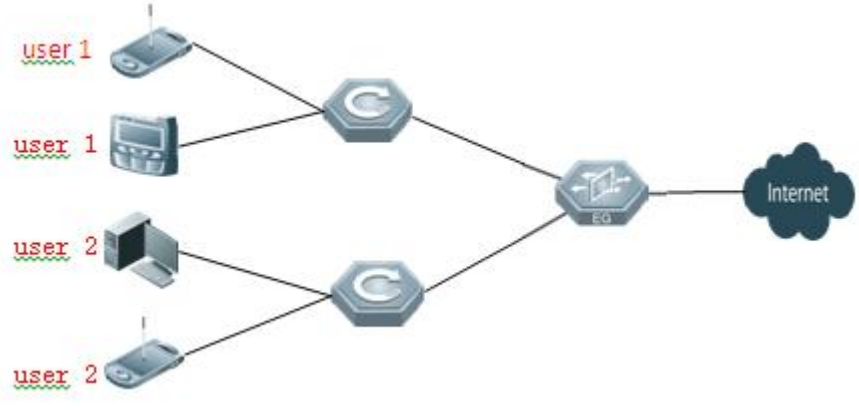
6.2.4 Flow Control Based on Account

Scenario

The bandwidth needs to be distributed based on accounts in some environments. Multiple terminals (such as pad, notebook computer and mobile phone) use the same account.

Flow control based on account can be configured in this scenario. For example, the user has two accounts: user 1 and user 2, and wishes to allocate 10 Mbps bandwidth to user 1 and 2 Mbps bandwidth to user 2, as shown in the following figure.

Figure 6-4



Deployment

Configure a flow control channel.

Configure a flow control policy.

Enable the account identification function.

6.3 Features

Basic Concepts

"Flow Control Group" and "Flow Control Tree"

FS egress gateway series products can enable the flow control function on the device WAN port: the flow control group is applied to an interface.

The flow control group contains the uplink flow control tree and downlink flow control tree, which control the uplink flow and downlink flow respectively. Some flow control channels are defined in the flow control tree to cache packets. Meanwhile, a series of flow control policies can be configured in the flow control group to indicate the packet behavior and accessed channel.

Flow Control Channel

The device caches and forwards packets according to properties of the flow control channel.

Assured Bandwidth (CIR)

CIR is the bandwidth limit allocated to the flow control channel.

Maximum Bandwidth (CIR)

PIR is the maximum bandwidth limit that can be occupied by the channel.

Maximum Bandwidth per IP Address (PER-CIR)

If the channel is configured as per-ip type, the maximum bandwidth per IP address - per-cir – can be set.

Flow Control Policy

The flow control policy is responsible for planning entry of the specified flow to the specified flow control channel. For example, a policy can be created so that the specified games can enter the key channel, and another policy can be created so that the specified P2P video can enter the suppression channel.

Flow Control Template

To make the configuration easier, a default configuration template is generated for flow control when the device starts without configuration. Such configuration templates can be revised, and the related revision does not lose after the templates are saved and device is restarted.

Overview

Feature	Description
Basic Function of Flow Control	Implements flow control
auto-pir Function	Ensures that the key application preempts bandwidth in time
P2P Precise Rate Limit	Implements precise rate limit on P2P traffic
Shared Pool Rate Limit	Allows adding flow control channels to the shared pool and affects packet scheduling of the added channels to implement more flexible flow control.

6.3.1 Basic Function of Flow Control

The basic function of flow control is flow control.

Working Principle

Flow control consists of the following steps:

25. Send packets to be forwarded by the device to different queues (known as "channels") for caching;
26. Schedule the packets in queues for sending according to channel properties.

The basic function of flow control consists of two parts: "flow control policy" and "flow control channel". The flow control channel is used to cache and forward packets actually. The flow control policy is used to decide whether packets should be discarded. If packets are not discarded, the flow control policy decides the channel that packets should enter.

Packet Classification and Caching

The device caches the packets to forward in the flow control channel according to the configured flow control policy.
At present, flow control settings support the following data flow classification method:
Classification based on Layer 2 (VID)
Classification based on user, where the user classification object contains the mapping relationship between user name and intranet source IP address
Classification based on network
Classification based on authentication object; all the authentication objects are matched by default
Classification based on application identification, supporting user-defined protocol classification objects
Classification based on VPN packet
Classification based on time segment
Classification based on account
The flow control policy is implemented based on the above class classification methods of data flows. Classification objects are combined to constitute the keywords of a policy rule, which then constitute the fundamental parts of a policy rule by adding the actions (such as blocking and rate limiting) to be adopted for the data flow by the policy rule. The collection of all the policy rules forms the flow control policy.

Packet Sending

The device forwards packets according to properties of the flow control channel. The flow control channel has a series of properties.

1. Parent channel. It corresponds to the bandwidth division model in the real environment, and the flow control channel finally forms a tree structure. Therefore, the flow control channel must have a parent channel (except for the root channel); meanwhile, multiple flow control channels can share a parent channel and are peers of each other.

If a flow control channel does not have a parent channel, it indicates that this channel is a root channel;

One flow control channel tree can have only one root channel.

2. Bandwidth. The flow control channel bandwidth consists of two parts: The commitment information rate (cir) and peak information rate (pir), where pir must be greater than or equal to cir. Here, cir is the bandwidth limit allocated to the flow control channel, and pir is the maximum bandwidth limit that can be occupied by the channel. The existence of pir allows the flow control channel to send packets with a bandwidth exceeding cir, implementing the so-called flexile bandwidth. The significance of flexible bandwidth lies in the full utilization of the bandwidth. For example, the egress bandwidth of a company is 10 Mbps, and the allocated

bandwidth of Department 1 of the company is as follows: 5 Mbps for cir and 10 Mbps for pir. When the egress bandwidth is not used by other departments, Department 1 can occupy the 10 Mbps bandwidth completely to the maximum.

3. Priority. Absolute priority is adopted for scheduling between flow control channels, and the channel with a high priority is always scheduled first, so the packet loss probability is lower in the case of congestion.

Flow control channel priorities 0 to 7 are supported, where priority 0 is the highest one, and priority 7 is the lowest one;

Note that the channel priority is not directly linked with the bandwidth borrowing effect.

4. Channel type. The flow control channel supports different scheduling queues and algorithms implemented inside, including the FIFO queue and fair queue. The FIFO queue is the simplest one. Incoming packets are added to the queue tail, and outgoing packets are obtained from the queue head to send packets in sequence.

As the name suggests, the fair queue ensures fairness of the packet sending opportunity. It applies to the situation with congestion and ensures that the connection of large flow will not occupy all the bandwidth and the connection of small flow also gets a packet sending opportunity. Currently flow control supports two types of fair queues: Per-net queue and Per-user queue.

Per-net queue is the fair queue based on network segment. It creates the corresponding number of queues according to the number of network segments configured by the user. Packets enter the corresponding queue based on the related network segment, and then packets are sent to all the queues in turn. To prevent a network segment from occupying an excessive bandwidth, Per-net queue can specify the committed bandwidth and peak bandwidth of each internal queue. The rate is limited for the intranet network segment by default, and reverse Per-net can be configured to limit the rate for the external network segment.

Per-user queue is the fair queue based on account. It creates the corresponding number of queues according to the number of accounts configured by the user. Packets enter the corresponding queue based on the related account, and then packets are sent to all the queues in turn. To prevent an account from occupying an excessive bandwidth, Per-user queue can specify the committed bandwidth and peak bandwidth of each account.

Related Configuration

Configuring a Flow Control Group

Some flow control templates exist in the device by default. An existing flow control group can be used as a template to copy a new configuration. Moreover, the bandwidth size can be updated and used to generate new configuration quickly according to the template or other flow control groups in the deployment phase:

flow-template copy Src_name Dst_name [bandwith_In_bandwith Out_bandwith [perpir-update]] [force]

If the flow control template cannot meet the user's requirement, the user can configure a flow control group:

5. Use the **flow-control** { *name* [**update bandwith_***In_bandwith Out_bandwith* [**perpir-update**]] } command to create a flow control group;

6. Use the **channel-tree** { **inbound** | **outbound** } command to create a flow control channel tree;

7. Use the **channel-group** *name* **parent** { **NULL** | *parent_name*} [**cir** *cir_num*] **pir** *pir_num* [**pri** *pri_num*] [ ] { **fifo** | { **per-net** [**per-mask** *mask*] | **per-user** } **per-pir** *ppir_num* [**limit** *limit_num*] [**session-limit** *session_limit_num*] [**reverse**] } command to create a flow control channel;

8. Use the **flow-rule** *num* [**vlan-group** *vlan-group-name*] [**subscriber** *subscriber-name*] [**auth-group** *auth-group-name*] [**network-group** *network-group-name*] [**app-group** *app-group-name*] **time-range** *time-rang-name* [**vpn**] and **flow-rule** *num* **action** { **drop** /**log-drop** /**pass** [**in-channel** *in-channel-name*] [**out-channel** *out-channel-name*] } [**default**] [**commet** *string*] command to create a flow control policy.

Enabling the Flow Control Function on the WAN Port

The flow control function is disabled by default on the WAN port.

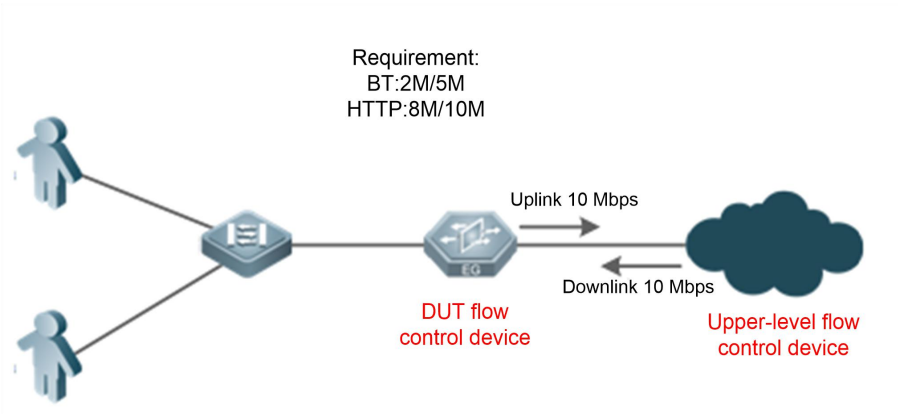
The **flow-policy** *name* command can be used to enable the flow control function on the WAN port, and the **no flow-policy** command can be used to cancel the application of a specific flow control group on the interface.

The flow control function must be enabled on the interface.

6.3.2 auto-pir Function

Working Principle

The auto-pir scenario is shown below:



The requirements for the DUT flow control device are as follows:

1. The BT assured bandwidth (CIR) is 2 Mbps, and the maximum bandwidth (PIR) is 5 Mbps;
2. The HTTP assured bandwidth (CIR) is 8 Mbps, and the maximum bandwidth (PIR) is 10 Mbps.

Note that the upper-level flow control device limits the rate of downlink flow to 10 Mbps in this scenario, and packet loss without difference is implemented for the excess flow. This scenario is of universal significance because the Internet Service Provider (ISP) assures the maximum bandwidth supported such as 2 Mbps and 10 Mbps when Internet is accessed for enterprises, schools and financial institutions.

During the test, BT downloading starts first to achieve the expected result: The maximum flow of 5 Mbps can be reached; then HTTP flow downloading starts. The expected result is that HTTP reaches the guaranteed 8 Mbps bandwidth and the BT flow is 2 Mbps, but the actual test result is that the BT flow is 5 Mbps and the HTTP flow is 5 Mbps. The reason analysis is as follows:

1) The upper-level flow control device limits the downlink to 10 Mbps and implements proportional packet loss without difference for BT and HTTP;

2) For the BT flow, a large proportion of bandwidth is preempted on the upper-level flow control device due to numerous connections and the large quantity of packets, leading to packet loss of the HTTP flow. Actually only 5 Mbps HTTP flow reaches the DUT device, so no more bandwidth can be preempted.

The PIR dynamic adjustment function identifies the above scenario: If the channel rate exceeds CIR provided that the total bandwidth is scarce, the PIR is reduced for the channel with the rate exceeding CIR. Take the above scenario as an example: The BT flow PIR is suppressed to 2 Mbps to reduce the downlink BT flow passing the DUT device from the original 5 Mbps to 2 Mbps, and the high packet loss rate urges the BT peer end to reduce the sending rate. Thus, the BT flow of upper-level flow control device is reduced greatly, and the HTTP flow occupies more bandwidth.

Related Configuration

Configuring auto-pir

This function is disabled on NPE products by default, but is enabled on gateway devices such as the EG, NBR and AG by default.

This **auto-pir enable** [**interval** *NUM* [**root-rate** *Percentage*]] [**exclude-pass**] command can be used to enable the PIR dynamic adjustment function of flow control channel tree. Use the **no auto-pir enable** command to disable the PIR dynamic adjustment function of flow control channel tree.

6.3.3 Shared Pool Rate Limit

Working Principle

The shared pool allows adding flow control channels and affecting packet scheduling of the channels to implement more flexible flow control. Shared pool involves the following two attributes:

Bandwidth

Bandwidth is the shared pool rate limit value. The shared pool of the normal type limits the rate of total traffic in all flow control channels. The shared pool of the Per-IP-type limits the rate of traffic of each client in all flow control channels.

Shared Pool Type

There are two shared pool types: normal and Per-IP. See preceding description for their definitions. Note the following for the shared pool in the per-ip type:

a. The limit on user quantity be configured, so as to block flows when the user quantity exceeds the limit.

b. Channels to be added to the shared pool in the per-ip type must be in the Per-net type, with the per-mask value being 32, namely, the per-ip type. In addition, the channel limit must be less than or equal to the shared pool limit.

Only a leaf channel and its parent channel (the two lowest layers of the flow control tree) can be added to shared pools, but they cannot be added to the same shared pool.

A shared pool supports up to 8 member channels. If a member channel is a non-leaf node, the number of its sub channels is less than or equal to 8.

If channels added to the shared pool are prioritized, those with higher priorities occupy all bandwidth of the shared pool in the worst case. Pay attention to the configuration effect.

The shared pool function is not supported on NPE products, but is supported on gateway devices such as the EG, NBR, and AG.

Related Configuration

No shared pool is configured by default.

Run the share-pool Name rate num1 [type { normal | per-ip [limit num2l }] command to configure a shared pool. Run the no share-pool Name command to delete a shared pool.

6.4 Configuration

Configuration	Description and Command
Configuring the Basic Function	(Mandatory) It is used to create a flow control group.

of Flow Control	**flow-control** { *name* [**update bandwith**_*In_bandwith Out_bandwith* [**perpir-update**]] }	Configures a flow control group
	channel-tree { inbound | outbound }	Creates a flow control channel tree
	channel-group *name* **parent** { **NULL** | *parent_name* } [**cir** *cir_num*] **pir** *pir_num* [**pri** *pri_num*] [ ] { **fifo** | { **per-net** [**per-mask** *mask*] | **per-user** } **per-pir** *ppir_num* [**limit** *limit_num*] [**session-limit** *session_limit_num*] [**reverse**] }	Creates a flow control channel
	flow-rule *num* [**vlan-group** *vlan-group-name*] [**subscriber** *subscriber-name*] [**auth-group** *auth-group-name*] [**network-group** *network-group-name*] [**app-group** *app-group-name*] **time-range** *time-rang-name* [**vpn**] **flow-rule** *num* **action** { **drop** / **log-drop** / **pass** [**in-channel** *in-channel-name*] [**out-channel** *out-channel-name*] } [**default**] [**commet** *string*]	Configures a flow control policy rule, which needs to be configured by two parts; the first half part indicates the policy rule keyword, and the last part indicates the policy rule action
	flow-policy *name*	Applies the flow control group to the WAN port
Configuring auto-pir	(Optional) It is used to enable the key flow to preempt bandwidth quickly when all the bandwidth is occupied.	
	auto-pir enable [**interval** *NUM* [**root-rate** *Percentage*]] [**exclude-pass**]	Enables the PIR dynamic adjustment function of flow control channel tree
Configuring Shared Pool Rate Limit	(Optical).It is used to allow adding flow control channels to the shared pool and affecting packet scheduling of the channels to implement more flexible flow control.	
	share-pool *Name* **rate** *num1* [**type** { **normal** | **per-ip** [**limit** *num2* **l** }]	Creates the shared pool.

6.4.1 Configuring the Basic Function of Flow Control

Configuration Effect

Create a flow control group and enable it on the interface to implement the basic flow control function.

Notes

If flow control based on application is configured, the application identification function needs to be enabled.

If flow control based on user is configured, the user identification function needs to be enabled.

If flow control based on time segment is configured, the corresponding time segment object needs to be configured.

If flow control based on account is configured, the account needs to be an authenticated user and Layer-2 and Layer-3 identification needs to be enabled.

Configuration Steps

Using the Template Copying Function

Optional.

Use the template copying function to get a flow control group through direct copying.

Creating a Flow Control Group

It is mandatory unless the template copying function is used.

A flow control group can be enabled on each WAN port.

Creating a Flow Control Tree

It is mandatory unless the template copying function is used.

Each flow control group contains the uplink flow control tree and downlink flow control tree, which control the uplink flow and downlink flow respectively.

Creating a Flow Control Channel

It is mandatory unless the template copying function is used.

Configure a flow control channel under the flow control tree. It is used to cache and forward packets.

Creating a Flow Control Policy

A flow control policy needs to be configured generally; otherwise, packets enter the default channel for forwarding.

If the flow control objects such as VLAN and application identification are specified in the flow control policy, the corresponding object needs to be created under the related module.

Enabling Flow Control on the Interface

Mandatory.

Verification

The policy effectiveness and channel rate can be checked to judge whether flow control takes effect.

Check the policy effectiveness.

Check the channel rate.

Related Commands

Copying a Template

Command	**flow-template copy** *Src_name Dst_name* [**bandwith_***In_bandwith Out_bandwith* [**perpir-update**]] [**force**]
Parameter Description	*Src_name*: Indicates the copied source flow control group, i.e., name of the flow control group used as a template. *Dst_name*: Indicates the name of the created flow control group, which cannot be the same as *Src_name*. *In_bandwith*: Indicates the expected downlink bandwidth size after update, in the input range from 500 kbps to 10000000 kbps; the downlink bandwidth size of source configuration group is accessed by default if no value is entered. *Out_bandwith*: Indicates the expected uplink bandwidth size after update, in the input range from 500 kbps to

	10000000 kbps; the uplink bandwidth size of source configuration group is accessed by default if no value is entered. **perpir-update:** When a value is entered, Per-PIR will always be adjusted proportionally along with the bandwidth; when no value is entered and the bandwidth is 10 Mbps greater than the reference bandwidth, Per-PIR will not be adjusted proportionally. **Force:** If the target flow control group already exists and **force** is not entered, copying will fail; if **force** is entered, the existing flow control group will be deleted before copying.
Command Mode	Global configuration mode
Usage Guide	-

Creating a Flow Control Group

Command	**flow-control** { *name* [**update bandwith_***In_bandwith Out_bandwith* [**perpir-update**]] }
Parameter Description	*name*: Indicates the name of the flow control group. *In_bandwith*: Indicates the expected downlink bandwidth size after update. *Out_bandwith*: Indicates the expected uplink bandwidth size after update. To create a flow control group, just execute **flow-control {***name***}**.
Command Mode	Flow-control mode
Usage Guide	-

Creating a Flow Control Tree

Command	**channel-tree** { **inbound | outbound** }
Parameter Description	**inbound:** Indicates the downlink flow control tree. **outbound:** Indicates the uplink flow control tree.
Command Mode	Privileged EXEC mode
Usage Guide	-

Creating a Flow Control Channel

Command	**channel-group** *name* **parent** { **NULL** | *parent_name*} [**cir** *cir_num*] **pir** *pir_num* [**pri** *pri_num*] [ ] { **fifo** | { **per-net** [**per-mask** *mask*] | **per-user** } **per-pir** *ppir_num* [**limit** *limit_num*] [**session-limit** *session_limit_num*] [**reverse**] }
Parameter Description	*name*: Indicates the name of the flow control group. **parent:** Indicates the parent channel of the created channel. **NULL:** The created channel is the root channel of the flow control tree if there is no parent channel. *parent_name*: Indicates the name of the parent channel of the created channel, which must be a created channel. **cir** *cir_num*: Indicates the acknowledge information rate, namely, the minimum assured bandwidth, in the input range from 100 kbps to 10000000 kbps; the parameter is 0 by default when no value is entered; bandwidth distribution is not committed when the bandwidth is scarce. **pir** *pir_num*: Indicates the peak information rate, namely, the maximum bandwidth that can be occupied, which

	must be greater than or equal to **cir**; the part exceeding **cir** is the size of bandwidth borrowed from the parent channel, in the input range from 100 kbps to 10000000 kbps. **pri** *pri_num*: Indicates the priority, in the input range from 0 to 7, where 0 indicates the highest priority and the channel with a higher priority will be first scheduled. **fifo:** indicates the FIFO queue. **per-net:** Indicates the fair queue of each network segment; the number of internal queues is not fixed, and the fair packet sending opportunity is realized based on the network segment; the parameter applies to the congested channel, and the following parameters need to be configured for it. **per-mask** *mask:* Indicates the network segment mask, in the input range from 1 to 32; 32 indicate the fair queue based on each IP address; the parameter is 32 by default if no value is entered. **per-user:** Indicates the fair queue per account; the number of internal queues is not fixed, and the fair packet sending opportunity is realized based on account; the parameter applies to the congested channel. **per-pir** *ppir_num*: Indicates the peak information rate of each network segment, namely, the maximum bandwidth that can be occupied, in the input range from 1 kbps to 10000000 kbps. **limit** *limit_num*: Indicates the number of limited network segments, in the input range from 1 to 65535; if no value is entered, the default value is accessed according to the total bandwidth size; 1000 is accessed when the total bandwidth is smaller than 100 Mbps; 10000 is accessed when the total bandwidth is greater than or equal to 100 Mbps. **session-limit** *session_limit_num*: Limits the number of connections of each network segment (IP address), in the input range from 1 to 65535; the number of connections of each IP address is not limited by default. **pool** *pool_name*: Indicates the name of the shared pool to which the configured flow control channel is added. The shared pool function is not supported by the NPE product, but is supported by gateway devices such as the EG, NBR, and AG. **reverse:**(Optical) Indicates reversed Per-net, implements rate limit on extranet IP segments, and implements rate limit on public IP segments for accessing branch devices in the VPN scenario. Forward Per-net is configured by default.
Command Mode	**channel-tree** configuration mode
Usage Guide	-

Creating a Flow Control Policy

Command	**flow-rule** *num* [**vlan-group** *vlan-group-name*] [**subscriber** *subscriber-name*] [**auth-group** *auth-group-name*] [**network-group** *network-group-name*] [**app-group** *app-group-name*] **time-range** *time-rang-name* [**vpn**] **flow-rule** *num* **action** {**drop** /**log-drop** /**pass** [**in-channel** *in-channel-name*] [**out-channel** *out-channel-name*] } [**default**] [**commet** *string*]
Parameter Description	num: Indicates the No. of flow control policy rule, in the input range from 1 to 8192. vlan-group-name: indicates the name of the vlan-group object associated with policy rule; "any" indicates matching any object. subscriber-name: Indicates the name of the subscriber object associated with policy rule; "any" indicates matching any object. *auth-group-name*: Indicates the name of the authentication object associated with policy rule; "any" indicates matching any authentication object.

	network-group-name: Indicates the name of the network-group object associated with policy rule; "any" indicates matching any object. app-group-name: Indicates the name of the app-group object associated with policy rule; "any" indicates matching any object. time-rang-name: Indicates the name of the time-rang object associated with policy rule. in-channel-name: Indicates the name of the in-channel channel associated with policy rule. out-channel-name: Indicates the name of the out-channel channel associated with policy rule. string: Indicates the comment of the policy rule. **disable:** Disables this policy rule. It is not disabled by default. **Vpn:** Indicates the configured VPN policy, which matches VPDN traffic only. A Non-VPN policy is configured by default. **default:** Default policy, at the lowest priority; for multiple default policies, the finest one will take effect first.
Command Mode	flow-control mode
Usage Guide	Configure a flow control policy rule, which needs to be configured by two parts; the first half part indicates the policy rule keyword, and the last part indicates the policy rule action.

Enabling Flow Control on the Interface

Command	**flow-policy** *name*
Parameter Description	*name*: Indicates the name of the flow control group.
Command Mode	Interface configuration mode
Usage Guide	-

Displaying Details of a Flow Control Policy Rule

Command	**show flow-control-policy rule** [**group** *name*]
Parameter Description	*name*: Indicates the name of the flow control group.
Command Mode	Privileged EXEC mode
Usage Guide	-

Displaying the Channel Rate

Command	**show flow-control** *Name* [**inbound | outbound**] **auto-pir**
Parameter Description	*Name*: Indicates the name of the flow control group.
Command Mode	Privileged EXEC mode
Usage Guide	-

Configuration Examples

Using a Template to Configure Flow Control Based on Application

Scenario	Business requirement of an Internet café: The egress bandwidth is 100 Mbps. Key applications such as web pages and games need to be guaranteed, and the P2P video requirement is not high.
Configuration Steps	● Copy a flow control group according to the Internet café template. ● Apply the copied flow control group to the interface. FS(config)#flow-template copy tpl-ibar Gi0/1 bandwith 100000 100000 FS(config)#int Gi0/1 FS(config-if-GigabitEthernet 0/1)#flow-policy Gi0/1
Verification	● Use the following two commands to perform check: ● show flow-control-policy rule Gi0/1: Use this command to check whether the policy takes effect. ● show flow-control Gi0/1 auto-pir: Use this command to check whether the channel rate is normal.

Configuring Flow Control Based on User

Scenario	The network egress bandwidth of a company is 10 Mbps. Three departments are defined in the company: department 1, department 2 and department 3, and the network segments are 192.168.1.0/24, 192.168.2.0/24 and 192.168.3.0/24, to which bandwidths 5 Mbps, 3 Mbps and 2 Mbps are allocated in turn.
Configuration Steps	● Create the uplink and downlink flow control channel trees respectively according to the actual requirement. ● Configure the configuration related to application identification and identify the flow of each department. ● Configure the flow control policy and decide the flow control channel corresponding to the flow of each department. ● Apply the flow control group to the WAN port.
	3. Configure the flow control group and flow control channel tree. FS# configure terminal #Create a flow control group. FS(config)# flow-control Corp #Create a flow control tree in the downlink direction. FS(config-flow-control)# channel-tree inbound FS(config-channel-tree)# channel-group root parent null cir 10000 pir 10000 pri 4 fifo FS(config-channel-tree)# channel-group department1 parent root cir 5000 pir 10000 pri 4 fifo FS(config-channel-tree)# channel-group department2 parent root cir 3000 pir 10000 pri 4 fifo FS(config-channel-tree)# channel-group department3 parent root cir 2000 pir 10000 pri 4 fifo

	FS(config-channel-tree)# exit #Create a flow control tree in the uplink direction. FS(config-flow-control)# channel-tree outbound FS(config-channel-tree)# channel-group root parent null cir 10000 pir 10000 pri 4 fifo FS(config-channel-tree)# channel-group department1 parent root cir 5000 pir 10000 pri 4 fifo FS(config-channel-tree)# channel-group department2 parent root cir 3000 pir 10000 pri 4 fifo FS(config-channel-tree)# channel-group department3 parent root cir 2000 pir 10000 pri 4 fifo FS(config-channel-tree)# exit FS(config-flow-control)# exit
B	4. Configure Layer-2 and Layer-3 object identification. FS# configure terminal #Enable the Layer-2 and Layer-3 object function. FS(config)# layer23 classify enable #Configure department identification. FS(config)# subscriber static name department1 parent / ip-subnet 192.168.1.0 255.255.255.0 FS(config)# subscriber static name department2 parent / ip-subnet 192.168.2.0 255.255.255.0 FS(config)# subscriber static name department3 parent / ip-subnet 192.168.3.0 255.255.255.0 #The time object does not support the **any** keyword and displays the defined **any** content. FS(config)# time-range any FS(config-time-range)# periodic Daily 0:00 to 23:59
C	5. Configure a flow control policy. FS# configure terminal FS(config)# flow-control Corp #Departments 1, 2 and 3 enter flow control channels department1, department2 and department3 respectively. FS(config-flow-control)# flow-rule 1 vlan-group any subscriber department1 network-group any app-group any time-rang any FS(config-flow-control)# flow-rule 1 action pass in-channel department1 out-channel department1 FS(config-flow-control)# flow-rule 2 vlan-group any subscriber department2 network-group any app-group any time-rang any FS(config-flow-control)# flow-rule 2 action pass in-channel department2 out-channel department2 FS(config-flow-control)# flow-rule 3 vlan-group any subscriber department3 network-group any app-group any time-rang any FS(config-flow-control)# flow-rule 3 action pass in-channel department3 out-channel department3
D	6. Apply the flow control group to the interface.

	FS# configure terminal FS(config)# interface GigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# flow-policy Corp
Verification	Use the following two commands to perform check: ● **show flow-control-policy rule** *Corp*: Use this command to check whether the policy takes effect. ● **show flow-control** *Corp* **auto-pir**: Use this command to check whether the channel rate is normal.

Common Errors

A flow control policy rule consists of the keyword part and behavior part, and a complete rule is formed only when two parts are configured. The behavior part cannot be configured when the keyword part is not configured. To make the configured policy take effect, first configure all the objects associated with the policy rule.

6.4.2 Configuring auto-pir

Configuration Effect

You can configure auto-pir so that the key flow can preempt bandwidth quickly when the full bandwidth is used.

Notes

N/A

Configuration Steps

Enable or disable auto-pir in channel-tree mode.

Verification

The related command can be used to display details of auto-pir, including whether this function is enabled, and the threshold size. This command is show flow-control Name auto-pir.

Related Commands

Configuring auto-pir

Command	**auto-pir enable** [**interval** *NUM* [**root-rate** *Percentage*]] [**exclude-pass**]
Parameter Description	*NUM*: Indicates the adjustment interval, in seconds. The parameter is 1 second by default if no value is configured, and the configuration range is from 1 to 3600. *Percentage*: Indicates the threshold of PIR suppression or restoration. **exclude-pass:** The **root-rate** threshold calculation includes the release flow by default. The pass flow is not included after the **exclude-pass** keyword is entered.
Command Mode	**channel-tree** configuration mode
Usage Guide	This function applies to the scenario where the flow control device of higher level exists. If the bandwidth occupation of point-to-point flow stays in a high position without going down and the bandwidth of other

	applications cannot be guaranteed, this function can be used. The root bandwidth utilization rate calculated here is the actual utilization rate, including the forwarded and discarded flow of flow control.

Displaying the auto-pir Information

Command	**show flow-control** *Name* [**inbound** | **outbound**] **auto-pir**
Parameter Description	*Name*: Indicates the name of the flow control group.
Command Mode	Privileged EXEC mode
Usage Guide	-

Configuration Examples

Enabling the Downlink auto-pir Function of Flow Control Group group1

Configuration Steps	● Configure the basic function of flow control. Details are omitted. ● Enable the inbound channel tree PIR regulation function of policy group group1.
	FS(config)# config FS(config)# flow-control group1 FS(config-flow-control)# channel-tree inbound FS(config-channel-tree)# auto-pir enable
Verification	Use the **show flow-control** ***group1*** **auto-pir** command to test whether auto-pir can take effect.

6.4.3 Configuring Shared Pool Rate Limit

Configuration Effect

Allow adding flow control channels to the shared pool and affect packet scheduling of the channels to implement more flexible flow control.

Notes

The shared pool function is not supported on the NPE product, but is supported on gateway devices such as the EG, NBR, and AG.

Configuration Steps

- Add specified channels to the shared pool in channel-tree mode.

Verification

Use the following command to display shared pool configuration information: show flow-control Name { inbound | outbound } [share-pool [pool-name]]

Related Commands

Creating Shared Pool

Command	**share-pool** *Name* **rate** *num1* [**type** { **normal** | **per-ip** [**limit** *num2*1 }]
Parameter Description	*Name*: Indicates the name of a shared pool. *num1*: Indicates the bandwidth of the created shared pool. **type:** Indicates the type of the created shared pool. This parameter is set to **normal** by default if no value is entered. **normal:** Indicates the normal type, which limits the total bandwidth rate of all users. **per-ip:** Indicates the per-ip type, which limits the bandwidth rate of each user. *num2:* Indicates the limit of user quantity of the shared pool in the per-ip type.
Command Mode	Channel tree configuration mode
Usage Guide	1. For the shared pool in the normal type, the bandwidth is limited based on all users of the channels added to the shared pool. That is, the total user bandwidth cannot exceed the configured rate. 2. For the shared pool in the per-ip type, the bandwidth is limited based on each user of the channels added to the shared pool. That is, the bandwidth of each user cannot exceed the configured rate. 3.User traffic is blocked when the limit of the shared pool in the per-ip type is exceeded. A limit value is generated automatically when no limit value is entered. 4.Channels added to the shared pool are prioritized. In a worst case, those with higher priorities occupy all bandwidth of the shared pool. This characteristic is applicable to scenarios with different service priorities.

Adding Channels to Shared Pool

Command	**channel-group** *name* **parent** { **NULL** | *parent_name* } [**cir** *cir_num*] **pir** *pir_num* [**pri** *pri_num*] [ ] { **fifo** | { **per-net** [**per-mask** *mask*] | **per-user** } **per-pir** *ppir_num* [**limit** *limit_num*] [**session-limit** *session_limit_num*] [**reverse**] }
Parameter Description	-
Command Mode	Channel tree configuration mode
Usage Guide	-

Configuration Example

Creating Shared Pool in normal Type with 1000kbps Bandwidth in the Inbound Flow Control Tree of Flow Control Group 1.

Configuration Steps	● #Create a shared pool.

	FS#config FS(config)#flow-control group1 FS(config-flow-control)# channel-tree inbound FS(config-channel-tree)# share-pool test rate 1000 type normal
Verification	Run the **show flow-control** *group1* **inbound share-pool** *test* to display the shared pool configuration information.

6.5 Monitoring

Displaying

Description	Command
Displays the details of flow control groups in the current device.	**show flow-control-policy group**
Displays details of the flow control policy rule.	**show flow-control-policy rule** [**group** *name*]
Displays the flow information of the specified flow control group.	**show flow-control** *Name* [**inbound** | **outbound**] **auto-pir**
Displays the flow control group configuration information. The configuration of all the flow control groups is displayed if no flow control group is specified.	**show flow-control** [*Name*]
Displays the flow control channel configuration information.	**show flow-control** *Name* { **inbound** | **outbound** } [**channel-group** *channel-name* [**detail**]]
Displays the shared pool configuration information.	**show flow-control** *Name* { **inbound** | **outbound** } [**share-pool** [*pool-name*]]

7 Configuring Flow Audit

7.1 Overview

Flow monitoring is a basic method of monitoring user behaviors, and can make user network applications visible to a network administrator. With flow monitoring, the network administrator can learn about different information, for example, IP session number, online duration of an IP address, Internet access duration of an IP application, traffic of a user, traffic of an application, application traffic of a user, traffic of an application group, traffic of an application type, and traffic of a user group. On the egress gateway, the flow audit function can be used to query traffic information.

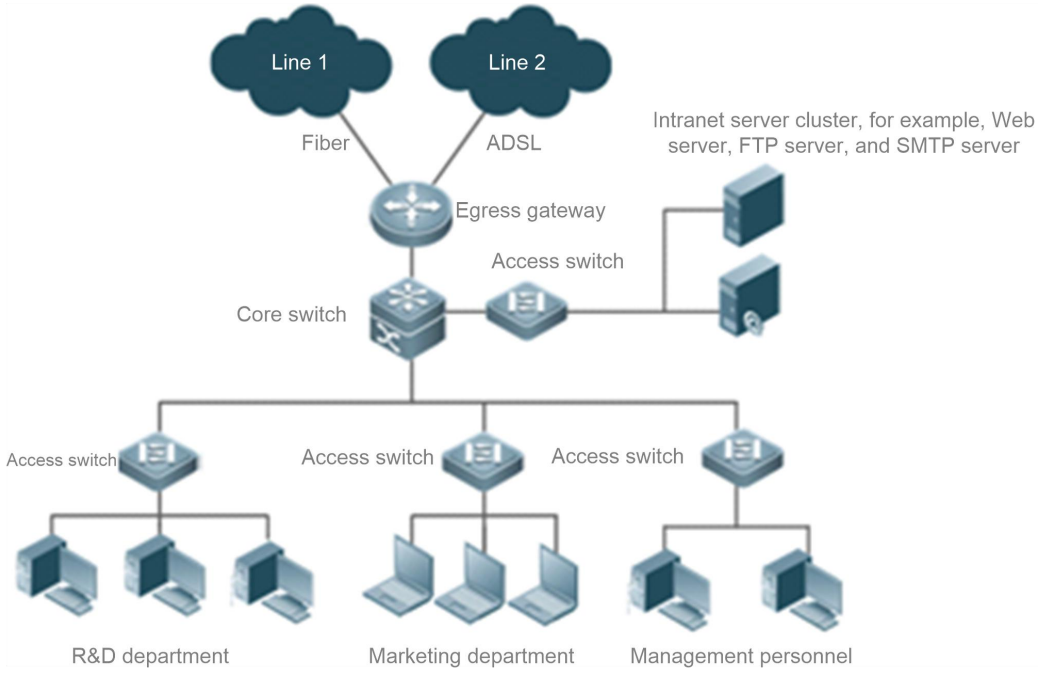
7.2 Applications

Application	Description
Deploying Egress Gateway	Deploys the flow monitoring and audit function on the egress gateway.

7.2.1 Deploying Egress Gateway

Scenario

Flow monitoring and audit does not impose requirement on topologies. Figure1- 1shows the typical network topology of an enterprise.
The following function relies on the flow audit function:
Application identification function
Figure 7- 1 Typical Application Scenario of Egress Gateway of an Enterprise Network



Remarks	Generally, different servers such as the Web server, FTP server, and SMTP server are deployed on an enterprise intranet. An enterprise is composed of many departments, such as the R&D department, marketing department, and management personnel, and a great number of network applications (for example, webpage browser and email) are connected to the Internet via the egress gateway.

Deployment

Basic NAT: Implement basic network address translation (NAT) to ensure that clients access the Internet normally.

Application identification: Indentify the application with traffic forwarding.

Flow control: Implement functions such as traffic guarantee of key applications in combination with APP-IDENTIFY.

L2/L3 application identification: Identify clients and client groups with traffic forwarding.

Multilink load balancing: Distribute data flows to multiple links to ensure proper utilization of bandwidth.

Flow audit: Measure different types of traffic passing the gateway based on clients or applications, to visualize the network traffic.

7.3 Features

7.3.1 Basic Concepts

Path

In bridge mode, a pair of bridges corresponds to one path. In gateway mode, a WAN interface corresponds to a path.

Application Details

Indicate an application subclass, for example, the QQ file transmission under the Tencent QQ.

Application Class

Example: key application and suppressed application

Application Group

Example: Instant messaging

User Group

In a user tree, the structure of user groups is as follows: root/level 1 user group/level 2 user group/level 3 user group/user.

Overview

Feature	Description
Flow Monitoring and Audit	Enables flow audit function.

7.3.2 Flow Monitoring and Audit

The flow audit function measures different types of traffic passing the gateway based on clients or applications to visualize the network traffic.

Working Principle

Flow monitoring and audit is implemented by measuring the number of packets obtained on the forwarding plane and the packet length. Packets can be measured by path, IP address, IP address application, user group, application details, application group, application class, interface, or VWAN, and stored to a database periodically.

Related Configuration

Enabling Flow Monitoring and Audit

This function is enabled by default.

Run the flow-audit enable command in global configuration mode to enable this function.

Run the no flow-audit enable command in global configuration mode to disable this function.

Configuring Flow Monitoring Mode of VPN

The flow monitoring of VPN is based on extranet IP addresses by default.

Run the flow-audit vpn {inside-ip | outside-ip} command to change the flow monitoring mode. The parameter inside-ip indicates intranet IP address-based monitoring, and the parameter outside-ip indicates extranet IP address-based monitoring.

To restore the default configuration, run the flow-audit vpn outside-ip command.

7.4 Configuration

Configuration	Description and Command	
Enabling Flow Monitoring and Audit	(Mandatory) It is used to enable flow audit.	
	flow-audit enable	Enables flow audit.
Configuring Storage Period of Historical Data	(Optional) It is used to configure the storage period of historical data.	
	flow-audit data-store *num*	Configures the storage period of table data (except the daily/weekly/monthly reports).
	flow-audit data-store day-report *num*	Configures the storage period of historical data of daily reports.
	flow-audit data-store week-report *num*	Configures the storage period of historical data of weekly reports.
	flow-audit data-store month-report *num*	Configures the storage period of historical data of monthly reports.
Configuring Report Generation Time	(Optional) It is used to configure the report generation time. Changing system time will result in exceptions.	
	flow-audit generate-report *hour*	Configures the report generation time. The 24-hour clock system is used.
Configuring Hard Disk Space Quota Available for Flow Monitoring	(Optional) It is used to configure the hard disk space quota available for flow audit.	
	flow-audit hard-disk-quota *percent*	Configures the hard disk space quota available for flow monitoring. The parameter **percent** indicates the hard disk space quota available for flow monitoring in relative to the total hard disk capacity, and the value ranges from 1 to 100.
Configuring Flow Monitoring	(Optional) It is used to configure the flow monitoring mode of VPN.	

Mode of VPN	**flow-audit vpn {inside-ip | outside-ip}**	Configures the flow monitoring mode of VPN. The parameter **inside-ip** indicates intranet IP address-based monitoring, and the parameter **outside-ip** indicates extranet IP address-based monitoring.

7.4.1 Enabling Flow Monitoring and Audit

Configuration Effect

Enable flow audit to allow measuring different types of traffic passing the egress gateway and displaying various traffic information.

Notes

The flow audit function is invalid if the flow monitoring and audit switch is disabled.
Flow monitoring and audit relies on the application identification and L2/L3 identification functions. If the functions are disabled, the flow monitoring and audit function cannot measure traffic based on applications or clients.

Configuration Steps

Run a command in global configuration mode to enable flow monitoring and audit.

Verification

Check the flow monitoring and audit status.

Related Commands

Enabling Flow Monitoring and Audit

Command	**flow-audit enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Enabling Flow Monitoring and Audit

Configuration Steps	Configure flow monitoring and audit on the egress gateway.
	FS# configure terminal FS(config)#flow-audit enable

Verification	● Check the flow monitoring and audit status.
	FS#show run | in flow-audit flow-audit enable

7.4.2 Configuring Storage Period of Historical Data

Configuration Effect

Configure a storage period to delete data once the storage period expires.

Notes

This function is optional.
All data will be lost if the system is upgraded from 10.x and modularized.
Traffic data collection frequency varies with the report type. For an hourly report, the collection frequency is five minutes. For a daily report, the collection frequency is half an hour. For a weekly report, the collection frequency is two hours. For a monthly report, the collection frequency is eight hours.
The flow audit function invalid if the flow monitoring and audit switch is disabled. Expired data will not be deleted.
The storage period of table data (except the daily/weekly/monthly reports) ranges from 10 days to 90 days. The default storage period is 60 days.
The storage period of historical data of daily reports ranges from 10 days to 90 days. The default storage period is 60 days.
The storage period of historical data of weekly reports ranges from 1 week to 52 weeks. The default storage period is 8 weeks.
The storage period of historical data of monthly reports ranges from 1 month to 12 months. The default storage period is 12 months.

Configuration Steps

Run a command in global configuration mode to configure the storage periods of different types of historical data.

Verification

Check the storage periods of different types of historical data.

Related Commands

Configuring Storage Period of Table Data (Except the Daily/Weekly/Monthly Reports)

Command	**flow-audit data-store** *num*
Parameter Description	num: Indicates the storage period of historical data. The value ranges from 10 days to 90 days.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Storage Period of Historical Data of Daily Reports

Command	**flow-audit data-store day-report** *num*

Parameter Description	num: Indicates the storage period of historical data. The value ranges from 10 days to 90 days.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Storage Period of Historical Data of Weekly Reports

Command	**flow-audit data-store week-report** *num*
Parameter Description	num: Indicates the storage period of historical data. The value ranges from 1 week to 52 weeks.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Storage Period of Historical Data of Monthly Reports

Command	**flow-audit data-store month-report** *num*
Parameter Description	num: Indicates the storage period of historical data. The value ranges from 1 month to 12 months.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Changing Storage Period of Table Data (Except Daily/Weekly/Monthly Reports) to 12 Days

Configuration Steps	Configure the storage period on the egress gateway.
	FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# flow-audit data-store 12
Verification	● Check the configuration.
	FS#show run | in flow-audit flow-audit enable flow-audit data-store 12

Changing Storage Period of Historical Data of Daily Reports to 12 Days

Configuration Steps	Configure the storage period on the egress gateway.
	FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# flow-audit data-store day-report 12
Verification	● Check the configuration.
	FS#show run | in flow-audit flow-audit enable flow-audit data-store day-report 12

Changing Storage Period of Historical Data of Weekly Reports to 12 Weeks

Configuration Steps	Configure the storage period on the egress gateway.
	FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# flow-audit data-store week-report 12
Verification	● Check the configuration.
	FS#show run | in flow-audit flow-audit enable flow-audit data-store week-report 12

Changing Storage Period of Historical Data of Monthly Reports to 8 Months

Configuration Steps	Configure the storage period on the egress gateway.
	FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# flow-audit data-store month-report 8
Verification	● Check the configuration.

	FS#show run | in flow-audit flow-audit enable flow-audit data-store month-report 8

7.4.3 Configuring Report Generation Time

Configuration Effect

Generate reports at the specified time.

Notes

The report generation function is invalid if the flow monitoring and audit switch is disabled. No report will be generated at the specified time.

Configuration Steps

Run a command in global configuration mode to configure the report generation time.

Verification

Check the report generation time.

Related Commands

Configuring Report Generation Time

Command	**flow-audit generate-report** *hour*
Parameter Description	*Hour*: Indicates the report generation time. The 24-hour clock system is used.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring Generation Time of Daily/Weekly/Monthly Reports as 12:00

Configuration Steps	Configure the report generation time on the egress gateway.
	FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# flow-audit generate-report 12
Verification	● Check the report generation time.

	FS#show run | in flow-audit flow-audit enable flow-audit generate-report 12

7.4.4 Configuring Hard Disk Space Quota Available for Flow Monitoring

Configuration Effect

Specify the hard disk space quota available for flow monitoring.

Notes

The hard disk space quota available for flow monitoring is 50% of the total capacity by default. The quota can be changed according to actual situation. The value ranges from 1 to 100.
If the flow monitoring data exceeds the available hard disk space allocated for flow monitoring, the gateway automatically deletes the earliest data to free the hard disk space.

Configuration Steps

Run a command in global configuration mode to configure the hard disk space quota available for flow monitoring.

Verification

Check the hard disk space quota available for flow monitoring.

Related Commands

Configuring Hard Disk Space Quota Available for Flow Monitoring

Command	**flow-audit hard-disk-quota** *percent*
Parameter Description	*percent*: Indicates the hard disk space quota available for flow monitoring in relative to the total hard disk capacity. The value ranges from 1 to 100.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Changing Hard Disk Space Quota to 80%

Configuration Steps	Configure the quota on the egress gateway.
	FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# flow-audit hard-disk-quota 80

Verification	● Check the quota configuration.
	FS#show run | in flow-audit flow-audit enable flow-audit hard-disk-quota 80

7.4.5 Configuring Flow Monitoring Mode of VPN

Configuration Effect

Specify a flow monitoring mode (extranet IP address-based or intranet IP address-based) of VPN according to actual audit requirements.

Notes

Flow monitoring of VPN is based on extranet IP addresses by default.

Verification

Check the flow monitoring mode of VPN.

Related Commands

Configuring Flow Monitoring Mode of VPN

Command	**flow-audit vpn** { **inside-ip** | **outside-ip** }
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring Headquarters as VPN Server End and Checking Traffic of Different Branches (Through VPN Dialup)

Configuration Steps	Perform the configuration on the egress gateway.
	FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# flow-audit vpn outside-ip
Verification	● Check the flow monitoring mode of VPN.

	FS#show run | in flow-audit flow-audit enable flow-audit flow-audit vpn outside-ip

Configuring Branches as VPN Client Ends and Changing Flow Monitoring to Be Based on Intranet IP Addresses to Check VPN Access of Each Employee

Configuration Steps	Perform the configuration on the egress gateway.
	FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# flow-audit vpn inside-ip
Verification	● Check the flow monitoring mode of VPN.
	FS#show run | in flow-audit flow-audit enable flow-audit vpn inside-ip

7.5 Monitoring

Displaying

Description	Command
Displays the total number of online IP addresses at the present time, in the past few hours, or at specified time period.	**show online statistics** { **global** | **interface** *interface-name* } [{ **detail** [**offset** *start-record* { **limit** *record-num* }] | **recent** *hour* | **minute interval** *begin-year begin-month begin-day begin-hour:begin-minute* **to** *end-year end-month end-day end-hour:end-minute* | [**month** | **week**] **time-interval** *begin-year begin-month begin-day begin-hour* **to** *end-year end-month end-day end-hour* | **day** *begin-year begin-month begin-day* [**hour-interval** *begin-hour1* **to** *end-hour1* [*begin-hour2* **to** *end-hour2*]] }]
Displays the Internet access duration and traffic information of the online IP addresses of the global system at the present time and at specified time period, as well as the Internet access duration and traffic information of a specified path.	**show online ip** { **global** | **interface** *interface-name*} [[**subscriber** *subscriber-name*] [**subscriber-group** *subscriber-group*] [**vip**] | { **by-auth** } [**auth-subs-group** *auth-group-name*] [**auth-subs** *auth-name*]]] [**ip** *ip-address*] [{ **minute-interval** *begin-year begin-month begin-day begin-hour: begin-minute* **to** *end-year end-month end-day end-hour:end-minute* | { [**month** | **week**] **day-interval** *begin-year begin-month begin-day* **to** *end-year end-month end-day* | **day** *begin-year begin-month begin-day* } [**hour-interva** l *begin-hour* **to** *end-hour* [*begin-hour2* **to** *end-hour2*]] }] [**order-by** { { **pass** | **drop** } { **upload** | **download** } | **ip** | **subscriber-group** | **subscriber** | **auth-subs-group** | **auth-subs** } { **desc** | **asc** } [**top** n]]

Displays the number of online IP addresses, Internet access duration of applications, and traffic information of the global system at the present time, as well as such information of a specified path.	**show online ip-application** { **global** | **interface** *interface-name* } [[**subscriber** *subscriber-name*] [**subscriber-group** *subscriber-group*] [**vip**] | { **by-auth** } [**auth-subs-group** *auth-group-name*] [**auth-subs** *auth-name*]] [**ip** *ip-address*] [**application** *application-name*] [**application-group** *application-group*] [**application-type** *application-type*] [**order-by** { { **pass** | **drop** } { **upload** | **download** } | **ip** | **subscriber-group** | **subscriber** | **auth-subs-group** | **auth-subs** | **application** } { **desc** | **asc** }] [**offset** *start –record* { **limit** record-num }]
Displays the traffic information of the global system at the present time, in the past few hours, or at specified time period, as well as such traffic information of a specified interface.	**show flowrate** { **global** | **interface** *interface-name* } [{ **recent** *hour* | **minute_interval** *begin-year begin-month begin-day begin-hour:begin-minute* **to** *end-year end-month end-day end-hour:end-minute* | [**month** | **week**] **time-interval** *begin-year begin-month begin-day begin-hour* **to** *end-year end-month end-day end-hour* | { [**month** | **week**] **day-interval** *begin-year begin-month begin-day* **to** *end-year end-month end-day* | **day** *begin-year begin-month begin-day* } [**hour-interval** *begin-hour* **to** *end-hour* [*begin-hour2* **to** *end-hour2*]] } [**detail**]]
Displays the user traffic statistics of the global system at the present time, in the past few hours, or at specified time period, as well as such user traffic statistics of a specified path.	**show flowrate ip** { **global** | { **interface** *interface-name*} [**by-vpn**] | **vwan** } [**subscriber-group** *subscriber-group* **by-group** | [[**subscriber-group** *subscriber-group*] [**subscriber** *subscriber-name*] [**vip**] | { **by-auth** } [**auth-subs-group** *auth-group-name*] [**auth-subs** *auth-name*]] [**ip** *ip-address*] [**application** *application-name*] [**application-group** *application-group*] [**application-type** *application-type*]] [{ **recent** *hour* | **minute-interval** *begin-year begin-month begin-day begin-hour:begin-minute* **to** *end-year end-month end-day end-hour: end-minute* | { [**month** | **week**] **day-interval** *begin-year begin-month begin-day* **to** *end-year end-month end-day* / **day** *begin-year begin-month begin-day* } [**hour-interval** *begin-hour1* **to** *end-hour1* [*begin-hour2* **to** *end-hour2*]] }] [**order-by** { { **pass** | **drop** } { **upload** | **download** } | **ip** | **subscriber-group** | **subscriber** | **auth-subs-group** | **auth-subs** } { **desc** | **asc** } [**top** *n* [**detail**]]] [{ **detail** | **by-user** }]
Displays the traffic information of applications, application groups, or application classes of the global system at the present time or at specified time period, as well as such traffic information of a specified path.	**show flowrate application** { **global** | **interface** *interface-name* | **vwan** } [[**subscriber** *subscriber-name*] [**subscriber-group** *subscriber-group*] | { **by-auth** } [**auth-subs-group** *auth-group-name*] [**auth-subs** *auth-name*]] [**ip** *ip-address*] [**application-group** *application-group*] [{ [**by-group**] | [**application-type** *application-type*] [{ **by-type** | **application** *application-name* }] }] [{ **recent** *hour* | **minute-interval** *begin-year begin-month begin-day begin-hour:begin-minute* **to** *end-year end-month end-day end-hour:end-minute* | { [**month** | **week**] **day-interval** *begin-year begin-month begin-day* **to** *end-year end-month end-day* | **day** *begin-year begin-month begin-day* } [**hour-interval** *begin-hour1* **to** *end-hour1* [*begin-hour2* **to** *end-hour2*] }] [**order-by** { { **pass** | **drop** } { **upload** | **download** } | **application** } { **desc** | **asc** } [**top** *n*]] [**detail**]
Displays the number of online IP addresses and application traffic information of the global system at the present time, as well as such information of a specified path.	**show flowrate ip-application** { **global** | { **interface** *interface-name* } [**by-vpn**] } [[**subscriber** *subscriber-name*] [**subscriber-group** *subscriber-group*] [**vip**] | { **by-auth** } [**auth-subs-group** *auth-group-name*] [**auth-subs** *auth-name*]] [**ip** *ip-address*] [**application** *application-name*] [**application-group** *application-group*] [**application-type** *application-type*] [**order-by** { { **pass** | **drop** } { **upload** | **download** } | **ip** | **application** | **subscriber-group** | **subscriber** | **auth-subs-group** | **auth-subs** } { **desc** | **asc** } [**top** *n*]]

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs the report generation switch.	**debug flow-audit flowrate-report**

8 Configuring Content Audit

8.1 Overview

The behavior audit function is mainly intended for egress networks of enterprises and schools. It is used to supervise online behaviors of intranet users, so as to prevent behaviors such as chatting, visiting work-irrelevant websites, speculating on stocks, playing games, visiting illegal BBS forums, and receiving and sending illegal mails during work time.

After enabling the behavior audit function, an egress device can prevent leakage of confidential information, guarantee information assets security, and ensure legal online behaviors to avoid legal risks.

The behavior audit function includes application control audit, URL access control audit, instant messaging (IM) filtering and audit, client mail filtering and audit, Web mail filtering and audit, forum posting behavior filtering and audit, search engine keyword filtering and audit, virtual identity audit, and URL redirection. URL access control audit supports domain name audit for the encrypted HTTPS flows.

The MSC product supports URL access control audit only. The whole NBR-E series supports all the preceding services. Other gateway products without a built-in memory and the ACE series support application control audit, URL access control audit, IM filtering and audit, and URL redirection. Other gateway products with a built-in memory support all the preceding services.

8.2 Application

Application	Description
Typical Behavior Audit Application Scenarios	Basic behavior audit scenarios and functions

8.2.1 Typical Behavior Audit Application Scenarios

Scenario

The behavior audit function mainly includes the following scenarios:

Application control audit: monitors network behaviors of applications, allows or blocks the corresponding application data flows, and audits control behaviors.

URL filtering and audit: monitors URL accesses, classifies and audits URL accesses from an intranet, and filters corresponding URL access behaviors.

URL redirection: namely Web page redirection. It redirects network requests of users, thus satisfying network access needs of the users.

Apart from common HTTP flows, audit and filtering on domain names are also supported for the encrypted HTTPS flows.

IM filtering and audit: audits accounts and chat records of the mainstream IM systems (such as QQ and MSN), and filters accounts.

Mail filtering and audit: audits mail sending and receiving, and filters information of the mainstream mail systems (such as Outlook and Foxmail). For the devices with a built-in memory, it saves attachments of mails.

Plugin audit: only audits QQ content.

Post file filtering and audit: Audits the files posted on the mainstream netdisks and filters the file names.

HTTP Post filtering and audit: Audits and filters the data sent by HTTP Post.

Web mail filtering and audit: audits mail sending and filters information of the mainstream Web mail systems (such as mail systems of Sina.com, 163.com and qq.com).

Web BBS filtering and audit: audits and filters the posted information of the mainstream Web BBS sites (such as tianya.com and mop.com) and micro blogs (such as Sina Microblog and Tencent Microblog).

Web search filtering and audit: audits search behaviors of users and filters search engine keywords of the mainstream Web search engine sites (such as Baidu.com and Google.com).

Virtual identity audit: audits account IDs and go-online/go-offline behaviors of the mainstream social applications (such as WeChat and Microblog).

Telnet filtering and audit: audits the fields of Telnet data flows, such as the intranet IP address, intranet port number, server IP address, server port number, and connect or disconnect action.

FTP filtering and audit: audits the names of files uploaded and downloaded through FTP, to block or audit the uploaded files.

Deployment

You can customize behavior audit policies as follows:

Customize a policy to represent a group of behavior audit rules.

Customize various behavior audit rules in a policy group based on the application, content, and time period.

Associate a policy group with a static user and an authenticated user separately to validate behavior audit policies.

8.3 Features

Basic Concepts

URL Class

Internet URLs can be classified into types such as military, news, sports, and the like based on Web page content. Currently, the system comes with certain URL class libraries, and you can classify URLs as required.

URL Object

A URL object contains a group of relevant URLs. You can represent URLs contained in URL objects via regular expressions, or add URL classes (system URL classes and user-defined URL classes) into the URL objects. With reference to the following description, you will find that a URL object actually serves as a collection for URL access control.

Differences between a URL class and a URL object are as follows:

A URL class is classified based on Web page content and cannot be directly applied to URL access control rules.

An URL object is generally a collection defined for URL rules, such as “URL whitelist”, and contains URL entries that may have no direct relation.

Keyword

A keyword is a phrase or a word group contained in a concerned online behavior.

Content Object

A content object includes a series of keywords and regular expressions. Similar to a URL object, a content object actually serves as a collection of keywords.

Rule

How a device monitors access behaviors from an intranet is determined by a series of content audit rules, such as application control rules, URL rules, IM rules, mail rules, Web BBS rules, Web mail rules, and Web search rules. Before monitoring access behaviors from an intranet, you must configure corresponding content audit rules as required based on conditions such as the application, content, and time period.

Policy Group

A policy group is a collection of rules, and represents a group of behavior audit rules. You can associate a policy group with a static user and an authenticated user separately to validate the behavior audit function for corresponding users.

Overview

Feature	Description
Application Control Audit	Internet access behaviors of users are audited or blocked based on application classes.
URL Audit	URL access behaviors of users are audited or blocked based on URL classes.
URL Redirection	Network requests of users are redirected, thus meeting network access requirements of users.
IM Audit	User behaviors of using IM are audited or blocked.
Mail Audit	User behaviors of sending and receiving mails via mail clients are audited or blocked.
Web BBS Audit	Forum posting behaviors of users are audited or blocked.
Web Mail Audit	User behaviors of sending Web mails are audited or blocked.
Web Search Audit	User behaviors of using search engines are audited or blocked.
Virtual Identity Audit	User behaviors of using social applications are audited.
Posted File Audit	Audits the files posted on the mainstream netdisks and filters the file names.
HTTP Post Audit	Audits and filters the data sent by HTTP Post.
Telnet Audit	IP addresses, port numbers, and behaviors of the Telnet client and server are audited or blocked.
FTP Audit	Names of the files transmitted through FTP are audited or blocked.

8.3.1 Application Control Audit

The application control audit function monitors network behaviors based on application classes, allows or blocks the corresponding application data flows according to the specified rules, and audits control behaviors.

Working Principle

The application control audit function monitors application data flows based on the application identification results. As a basic function module on the egress device, APP-IDENTIFY analyzes packet payload and traffic characteristics of data flows to obtain the application protocol types of the data flows.

An application control audit rule is included in a policy group and can be used to specify an application data flow control and audit manner. A rule is a free combination of conditions such as a time object representing a validity time period, an application group name representing a to-be-controlled application type, information about whether to allow or block a data flow, and information about whether audit is required. Rules are prioritized.

Policy groups are prioritized, which can be associated with static users and authenticated users. The application control audit function matches a final valid rule according to the priorities of policy groups and rules, and monitors and audits Internet access behaviors of the specified users.

For the gateway device with a built-in memory, audit records are saved on the devices and you can display details and statistics in the application control audit records via corresponding show commands.

When audit information is sent to an external log server, you can determine not to save audit records on the device to reduce device load.

Related Configuration

Configuring Application Control Audit Rules

No application control audit rule is configured by default, and the application control audit function is automatically disabled.

Run the app-rule command to configure an application control audit rule. The application control audit function is automatically enabled after the rule is validated.

Rule parameters determine a manner for monitoring and auditing Internet access behaviors.

Displaying Application Control Audit Information

By default, audit records can be saved on the device for 60 days.

Run the show app-audit command to display details and statistics of application control audit records.

You can specify the time range and filtering conditions to display the corresponding audit records.

When audit information is sent to an external log server, you can run the no content-audit write-db app-control command to disable writing of application control audit information into the local memory.

8.3.2 URL Audit

The URL audit function is used to monitor URL accesses, classify and audit URL accesses from an intranet, and filter corresponding URL access behaviors of designated users.

Working Principle

URL refers to Uniform Resource Locator, and is also called Web page address. Internet URLs can be classified into types such as military, news, sports, and the like based on Web page content. Currently, the system comes with a URL class library that includes more than 50 classes. You can further self-define URL classes as required.

The URL audit function can identify URL information contained in an HTTP header of a data flow, match an identified URL according to system URL classes and user-defined URL classes to determine a class to which the URL belongs, and perform audit and filtering according to URL rules.

The URL audit function can also identify the domain names included in the encrypted HTTPS Web page data flows. The identified domain names are matched according to the default and self-defined URL classes and thus the domain name classes are determined. Then, the domain names are audited and filtered according to URL rules.

A URL audit rule is included in a policy group and can be used to specify a URL access control and audit manner. A rule is a free combination of conditions such as a time object representing a validity time period, a URL object representing a to-be-controlled URL class, information about whether to allow or block a data flow, and information about whether audit is required. Rules are prioritized.

Policy groups are also prioritized and can be associated with static users and authenticated users. The URL audit function matches a final valid rule according to priorities of policy groups and rules, and monitors and audits URL access behaviors of specified users.

For the gateway device with a built-in memory, audit records are saved on the device and you can display details, statistics, website ranks in the URL audit records via corresponding show commands.

When audit information is sent to an external log server, you can determine not to save audit records on the device to reduce device load.

Related Configuration

Configuring URL Audit Rules

No URL audit rule is configured by default, and the URL audit function is automatically disabled.

Run the url-rule command to configure a URL audit rule. The URL audit function is automatically enabled after the rule is validated.

Rule parameters determine a manner for monitoring and auditing URL access behaviors.

URL audit rules are valid to common Web page browsing only. To apply URL audit rules to the HTTPS encrypted data flows, enable HTTPS domain name audit. By default, HTTPS domain name audit is disabled.

Displaying URL Audit Information

By default, audit records can be saved on the device for 60 days.
Run the show url-audit command to display details, statistics, and website ranks in URL audit records. Common website audit records are consistent with HTTPS encrypted website audit records and URL information is distinguished by http:// and https://.
You can specify the time range and filtering conditions to display the corresponding audit records.
When audit information is sent to an external log server, you can run the no content-audit write-db url command to disable writing of URL audit information into the local memory.

8.3.3 URL Redirection

The URL redirection function, namely Web page redirection, redirects network requests of users, thus satisfying network access needs of users.

Working Principle

The URL redirection function can identify the URL information contained in the HTTP header of data flows and match the URL based on the URL redirection rule. If the URL matches the URL redirection rule, the user request is redirected to another website according to the URL redirection rule.
The URL redirection rule is included in a policy group. It can redirect the request for accessing website A to website B and specify the validity time period. Rules are prioritized.
Policy groups can be associated with static users and authenticated users. NBR products of NetBar type can also be associated with the self-defined user groups. Policy groups are also prioritized.
The URL redirection function matches a final valid rule according to priorities of policy groups and rules, and redirects website access of specified users.

Related Configuration

Configuring URL Redirection Rules

No URL redirection rule is configured by default, and the URL redirection function is automatically disabled.
Run the url-redirect-rule command to configure a URL redirection rule. The URL redirection function is automatically enabled after the rule is validated.
Rule parameters determine the user object and validity time period for URL redirection.

8.3.4 IM Audit

The IM audit function audits accounts and chat records of the mainstream IM systems (such as QQ and MSN), and filters accounts.

Working Principle

The MSN audit function audits accounts and chat records. The IM audit function can identify the account information and chat record information carried in the MSN data flows, and audit them. By blocking the data flows of the specified MSN account, the IM audit function filters accounts. By matching key words of chat records, the IM audit function blocks the corresponding data flows, and thus filtering chat records.
The QQ audit function audits accounts. QQ chat records are encrypted. At present, content filtering and audit is not supported. (The

message parameter of the QQ rule in the configuration command cannot be configured.) The QQ audit function can identify go-online/go-offline behaviors of QQ accounts on PCs and online behaviors of QQ accounts on mobile terminals, and can audit these behaviors. By blocking the data flows of the specified QQ accounts, the QQ audit function filters accounts.

An IM audit rule is included in a policy group and can be used to specify an IM access control and audit manner. A rule is a free combination of conditions such as a time object representing a validity time period, class of a to-be-controlled IM, account and keyword of a to-be-controlled IM, information about whether to allow or block a data flow, and information about whether audit is required. Rules are prioritized.

Policy groups are prioritized, which can be associated with static users and authenticated users. The IM audit function matches a final valid rule according to priorities of policy groups and rules, monitors and audits IM access of specified users.

For the gateway device with a built-in memory, audit records are saved on the device and you can display details and statistics in the IM audit records via corresponding show commands.

When audit information is sent to an external log server, you can determine not to save audit records on the device to reduce device load.

Related Configuration

➘ Configuring IM Audit Rules

No IM audit rule is configured by default, and the IM audit function is automatically disabled.

Run the im-rule command to configure an IM audit rule. The IM audit function is automatically enabled after the rule is validated.

Rule parameters determine a manner for monitoring and auditing IM access behaviors.

➘ Displaying IM Audit Information

By default, audit records can be saved on the device for 60 days.

Run the show im-audit command to display details, statistics, and website ranks in IM audit records.

You can specify the time range and filtering conditions to display the corresponding audit records.

When audit information is sent to an external log server, you can run the no content-audit write-db im command to disable writing of IM audit information into the local memory.

8.3.5 Mail Audit

The mail audit function audits mail sending and receiving and filters information of the mainstream mail systems (such as Outlook and Foxmail), and saves attachments of mails on the devices.

Working Principle

The mail audit function is to parse the unencrypted SMTP and POP3 data flows, and identify senders, receivers, subjects, bodies, and attachments in the data flows. By matching and auditing keywords in the information based on rules, the mail audit function determines whether to allow or block the data flows, thus auditing mail sending/receiving and filtering information.

A mail audit rule is included in a policy group and can be used to specify a mail access control and audit manner. A rule is a free combination of conditions such as a time object representing a validity time period, mail data flow direction, a content object representing a keyword, information about whether to allow or block a data flow, and information about whether audit is required. Rules are prioritized.

Policy groups are prioritized, which can be associated with static users and authenticated users. The mail audit function matches a final valid rule according to priorities of policy groups and rules, monitors and audits mail access of specified users.

For the gateway device with a built-in memory, audit records are saved on the device and you can display details, statistics, and attachments in the mail audit records via corresponding show commands.

When audit information is sent to an external log server, you can determine not to save audit records on the device to reduce device load.

Related Configuration

Configuring Mail Audit Rules

No mail audit rule is configured by default, and the mail audit function is automatically disabled.

Run the mail-rule command to configure a mail audit rule. The mail audit function is automatically enabled after the rule is validated.

Rule parameters determine a manner for monitoring and auditing mail access behaviors on the clients.

Displaying Mail Audit Information

By default, audit records can be saved on the device for 60 days.

Run the show mail-audit command to display details, statistics, and attachments in mail audit records.

You can specify the time range and filtering conditions to display the corresponding audit records.

When audit information is sent to an external log server, you can run the no content-audit write-db mail command to disable writing of mail audit information into the local memory.

8.3.6 Web BBS Audit

The Web BBS audit function audits and filters the posted information on the mainstream Web BBS sites (such as tianya.com and mop.com) and micro blogs (such as Sina Microblog and Tencent Microblog).

Working Principle

The Web BBS audit function is to parse the unencrypted HTTP data flows that include forum posts or micro blog posts, and identify subjects and bodies carried in the data flows. By matching and auditing keywords in the information based on the rules, the mail audit function determines whether to allow or block the data flows, thus auditing and filtering the posted information. At present, the Web BBS audit function does not support the micro blog clients (such as Sina Microblog clients and Tencent Microblog clients) on mobile terminals.

A Web BBS audit rule is included in a policy group and can be used to specify a Web BBS access control and audit manner. A rule is a free combination of conditions such as a time object representing a validity time period, a content object representing a keyword, information about whether to allow or block a data flow, and information about whether audit is required. Rules are prioritized.

Policy groups are prioritized, which can be associated with static users and authenticated users. The Web BBS audit function matches a final valid rule according to priorities of policy groups and rules, monitors and audits Web BBS access of specified users.

For the gateway device with a built-in memory, audit records are saved on the device and you can display details and statistics in the Web BBS audit records via corresponding show commands.

When audit information is sent to an external log server, you can determine not to save audit records on the device to reduce device load.

Related Configuration

Configuring Web BBS Audit Rules

No Web BBS audit rule is configured by default, and the Web BBS audit function is automatically disabled.

Run the web-bbs-rule command to configure a Web BBS audit rule. The Web BBS audit function is automatically enabled after the rule is validated.

Rule parameters determine a manner for monitoring and auditing Web BBS access behaviors on the clients.

Displaying Web BBS Audit Information

By default, audit records can be saved on the device for 60 days.

Run the show web-bbs-audit command to display details and statistics of Web BBS audit records.

You can specify the time range and filtering conditions to display the corresponding audit records.
When audit information is sent to an external log server, you can run the no content-audit write-db web-bbs command to disable writing of Web BBS audit information into the local memory.

8.3.7 Web Mail Audit

The Web mail audit function audits mail sending and filters information on the mainstream Web mail systems (such as mail systems of Sina.com, 163.com and qq.com). It also saves attachments of mails on the devices.

Working Principle

The Web mail audit function is to parse the unencrypted HTTP data flows that contain the mail sending information, and identify senders, receivers, subjects, bodies, and attachments carried in the data flows. By matching and auditing keywords in the information based on the rules, the Web mail audit function determines whether to allow or block the data flows, thus auditing mail sending and filtering information. At present, the Web mail audit function cannot audit mail receiving.
A Web mail audit rule is included in a policy group and can be used to specify a Web mail access control and audit manner. A rule is a free combination of conditions such as a time object representing a validity time period, a content object representing a keyword, information about whether to allow or block a data flow, and information about whether audit is required. Rules are prioritized.
Policy groups are prioritized, which can be associated with static users and authenticated users. The Web mail audit function matches a final valid rule according to priorities of policy groups and rules, monitors and audits Web mail access of specified users.
For the gateway device with a built-in memory, audit records are saved on the device and you can display details, statistics, and attachments in the audit records via corresponding show commands.
When audit information is sent to an external log server, you can determine not to save audit records on the device to reduce device load.

Related Configuration

➘ Configuring Web Mail Audit Rules

No Web mail audit rule is configured by default, and the Web mail audit function is automatically disabled.
Run the web-mail-rule command to configure a Web mail audit rule. The Web mail audit function is automatically enabled after the rule is validated.
Rule parameters determine a manner for monitoring and auditing Web mail access behaviors on the clients.

➘ Displaying Web Mail Audit Information

By default, audit records can be saved on the device for 60 days.
Run the show web-mail-audit command to display details, statistics, and attachments in audit records.
You can specify the time range and filtering conditions to display the corresponding audit records.
When audit information is sent to an external log server, you can run the no content-audit write-db web-mail command to disable writing of Web mail audit information into the local memory.

8.3.8 Web Search Audit

The Web search audit function audits search behaviors of users and filters search engine keywords of the mainstream Web search engine sites (such as Baidu.com and Google.com).

Working Principle

The Web search audit function is to identify the corresponding search keywords in the URLs that belong to a search engine based on the

identified URL information. It matches and audits the keywords in the URL information based on the rules, determines whether to allow or block the corresponding data flows, audits search behaviors of users, and filters information.

A Web search audit rule is included in a policy group and can be used to specify a Web search access control and audit manner. A rule is a free combination of conditions such as a time object representing a validity time period, a content object representing a keyword, information about whether to allow or block a data flow, and information about whether audit is required. Rules are prioritized.

Policy groups are prioritized, which can be associated with static users and authenticated users. The Web search audit function matches a final valid rule according to priorities of policy groups and rules, monitors and audits Web search access of specified users.

For the gateway device with a built-in memory, audit records are saved on the device and you can display details and statistics in the Web search audit records via corresponding show commands.

When audit information is sent to an external log server, you can determine not to save audit records on the device to reduce device load.

Related Configuration

Configuring Web Search Audit Rules

No Web search audit rule is configured by default, and the Web search audit function is automatically disabled.

Run the web-search-rule command to configure a Web search audit rule. The Web search audit function is automatically enabled after the rule is validated.

Rule parameters determine a manner for monitoring and auditing Web search behaviors on the clients.

Displaying Web Search Audit Information

By default, audit records can be saved on the device for 60 days.

Run the show web-search-audit command to display details and statistics of Web search audit records.

You can specify the time range and filtering conditions to display the corresponding audit records.

When audit information is sent to an external log server, you can run the no content-audit write-db web-search command to disable writing of Web search audit information into the local memory.

8.3.9 Virtual Identity Audit

The virtual identity audit function audits account IDs and nicknames of the mainstream social applications (such as WeChat and Microblog).

Working Principle

The virtual identity audit function can audit account IDs. It can identify and audit go-online/go-offline behaviors of accounts.

For the gateway device with a built-in memory, audit records are saved on the device and you can display details and statistics in the virtual identity audit records via corresponding show commands.

When audit information is sent to an external log server, you can determine not to save audit records on the device to reduce device load.

Related Configuration

Configuring Virtual Identity Audit Rules

No virtual identity audit rule is configured by default, and the virtual identity audit function is automatically disabled.

Run the vid-rule command to enable virtual identity audit.

Rule parameters determine a manner for monitoring and auditing virtual identity access behaviors.

Displaying Virtual Identity Audit Information

By default, audit records can be saved on the device for 60 days.
Run the show vid-audit command to display details, statistics, and website ranks in virtual identity audit records.
You can specify the time range and filtering conditions to display the corresponding audit records.

8.3.10 QQ Chat Audit

The QQ chat audit function audits the chats of QQ users on the client. A plug-in is required on the client to monitor the QQ software behavior.

Working Principle

The plug-in on the client sends the audited QQ chat information through UDP to the device for recording.

Related Configuration

Configuring Plug-in-based Audit Rules

No plug-in-based audit rule is configured by default, and the plug-in-based audit function is automatically disabled.
Run the plugin-rule command to configure a plug-in-based audit rule. The plug-in-based audit function is automatically enabled after the rule is validated.

Displaying Plug-in-based Audit Information

By default, audit records can be saved on the device for 60 days.
Run the show plugin-audit command to display details and statistics of plug-in-based audit records.
You can specify the time range and filtering conditions to display the corresponding audit records.
When audit information is sent to an external log server, you can run the no content-audit write-db plugin command to disable writing of plug-in-based audit information into the local memory.

8.3.11 Posted File Audit

The posted file audit function audits the files posted on the mainstream netdisks (such as Baidu Wenku and NetEase Netdisk) and filters the file names.

Working Principle

The posted file audit function is used to parse the HTTP data flows of uploaded files, and identify file names and file content from the data flows. Keywords are matched and audited based on the rules, to allow or block the data flows. In this way, the posted files are audited and filtered. At present, the posted file audit function is unavailable on mobile terminals.
A posted file audit rule is included in a policy group and can be used to specify a posted file access control and audit manner. A rule is a free combination of conditions such as a time object representing a validity time period, a content object representing a keyword, information about whether to allow or block a data flow, and information about whether audit is required. Rules are prioritized.
Policy groups are prioritized, which can be associated with static users and authenticated users. The posted file audit function matches a final valid rule according to priorities of policy groups and rules, and monitors and audits posted file access of specified users.
For the gateway device with a built-in memory, audit records are saved on the device and you can display details and statistics in the audit records via corresponding show commands.
When audit information is sent to an external log server, you can determine not to save audit records on the device to reduce device load.

Related Configuration

Configuring Posted File Audit Rules

No posted file audit rule is configured by default, and the posted file audit function is automatically disabled.

Run the postfile-rule command to configure a posted file audit rule. The posted file audit function is automatically enabled after the rule is validated.

Rule parameters determine a manner for monitoring and auditing posted file behaviors on the clients.

Displaying Posted File Audit Information

By default, audit records can be saved on the device for 60 days.

Run the show postfile-audit command to display details and statistics of posted file audit records.

You can specify the time range and filtering conditions to display the corresponding audit records.

When audit information is sent to an external log server, you can run the no content-audit write-db postfile command to disable writing of posted file audit information into the local memory.

8.3.12 HTTP Post Audit

The post audit function audits and filters the posted information on the mainstream Web BBS sites (such as tianya.com and mop.com) and micro blogs (such as Sina Microblog and Tencent Microblog).

Working Principle

The post audit function is used to parse all the unencrypted HTTP post data flows, and identify the posted HTTP information from the data flows. Keywords in the data flows are matched and audited based on the rules, to allow or block the data flows. In this way, the posted information is audited and filtered.

A post audit rule is included in a policy group and can be used to specify a post access control and audit manner. A rule is a free combination of conditions such as a time object representing a validity time period, a content object representing a keyword, information about whether to allow or block a data flow, and information about whether audit is required. Rules are prioritized.

Policy groups are prioritized, which can be associated with static users and authenticated users. The post audit function matches a final valid rule according to priorities of policy groups and rules, and monitors and audits post access of specified users.

For the gateway device with a built-in memory, audit records are saved on the device and you can display details and statistics in the audit records via corresponding show commands.

When audit information is sent to an external log server, you can determine not to save audit records on the device to reduce device load.

Related Configuration

Configuring Post Audit Rules

No post audit rule is configured by default, and the post audit function is automatically disabled.

Run the post-rule command to configure a post audit rule. The post audit function is automatically enabled after the rule is validated.

Rule parameters determine a manner for monitoring and auditing HTTP post behaviors.

Displaying Post Audit Information

By default, audit records can be saved on the device for 60 days.

Run the show post-audit command to display details and statistics of post audit records.

You can specify the time range and filtering conditions to display the corresponding audit records.

When audit information is sent to an external log server, you can run the no content-audit write-db post command to disable writing of

post audit information into the local memory.

8.3.13 Encryption-type Audit

The encryption-type audit function audits the SSL-encrypted traffic, covering the applications using HTTPS such as Web BBS, Web mail, Web search, virtual identity, and posted file.

Working Principle

The encryption-type audit function is used to obtain the plaintext traffic of users through the SSL proxy function and perform the preceding audit. After the function is enabled, the content audit module learns the DNS parsing results of various applications and determines the data flows that need the SSL proxy. Because the SSL proxy needs to encrypt/decrypt data flows using FS's SSL certificates, it is necessary to install SSL root certificates on the clients to avoid the failure of some applications caused by untrusted certificates.

Related Configuration

Enabling Encryption-type Audit

By default, the encryption-type audit function is disabled.
In the default audit policy, run the ssl-audit command to enable the encryption-type audit function, so that the function is validated in combination with the audit policies of various applications such as Web BBS, Web mail, Web search, virtual identity, and posted file.
Display the encryption-type audit results in the same way as those of the preceding applications.

8.3.14 Blocked Information Real-time Statistics Collection

The blocked information real-time statistics collection function collects statistics of the blocked audit information in real time.

Working Principle

The blocked information real-time statistics collection function is used to audit behaviors, match blocking policies, and collect statistics of the audit records before the records are stored in the database.

Related Configuration

Enabling Blocked Information Real-time Statistics Collection

This function is enabled by default.

8.3.15 Telnet Audit

The Telnet audit function audits the fields of Telnet data flows, such as the intranet IP address, intranet port number, server IP address, server port number, and connect or disconnect action.

Working Principle

The Telnet audit function is used to obtain the Telnet traffic and perform the preceding audit. After this function is enabled, you can obtain the IP addresses, port numbers, and behaviors of the Telnet client and server through data flows.

Related Configuration

Enabling Telnet Audit

By default, the Telnet audit function is disabled.

Run the telnet-rule command to configure a Telnet audit rule. The Telnet audit function is automatically enabled after the rule is validated.

Rule parameters determine a manner for monitoring and auditing Telnet behaviors.

Displaying Telnet Audit Information

Run the show telnet-audit command to display details and statistics of Telnet audit records.

You can specify the time range and filtering conditions to display the corresponding audit records.

You can run the no content-audit write-db telnet command to disable writing of Telnet audit information into the local memory.

8.3.16 FTP Audit

The FTP audit function audits and filters the file names transmitted through FTP and the uploaded files.

Working Principle

The FTP audit function is used to parse the FTP data flows of uploaded and downloaded files, and identify file names from the data flows. Keywords in the file names are matched and audited based on the rules, to allow or block the data flows. In this way, the file names uploaded or download through FTP and the uploaded file content are audited and filtered.

An FTP audit rule is included in a policy group and can be used to specify an FTP access control and audit manner. A rule is a free combination of conditions such as a time object representing a validity time period, an object representing a file name keyword, information about whether to allow or block a data flow, and information about whether audit is required. Rules are prioritized.

Policy groups are prioritized, which can be associated with static users and authenticated users. The FTP audit function matches a final valid rule according to priorities of policy groups and rules, and monitors and audits FTP access of specified users.

For the gateway device with a built-in memory, audit records are saved on the device and you can display details and statistics of the audit records via corresponding show commands.

The FTP file audit function is disabled by default. When it is enabled, the uploaded file content is audited.

You can determine not to save audit records on the device to reduce device load.

Related Configuration

Enabling FTP Audit

By default, the FTP audit function is disabled.

Run the ftp-rule command to configure an FTP audit rule. The FTP audit function is automatically enabled after the rule is validated.

Rule parameters determine a manner for monitoring and auditing FTP behaviors.

Displaying FTP Audit Information

Run the show ftp-audit command to display details and statistics of FTP audit records.

You can specify the time range and filtering conditions to display the corresponding audit records.

When audit information is sent to an external log server, you can run the no content-audit write-db ftp command to disable writing of FTP audit information into the local memory.

8.3.17 File Filtering

The file filtering function filters the file types and file names of Web mail attachments, Web BBS attachments, and posted files.

Working Principle

The posted file, Web mail, and BBS mail have their own attachment name filtering rules, which are conflicted with refined file control. To resolve the conflict, keep the priorities of module rules higher than that of refined file control.

Related Configuration

Enabling File Filtering

The file filtering function is disabled by default.
Run the file-rule command to configure a file filtering rule. The file filtering function is automatically enabled after the rule is validated.
Rule parameters determine a manner for monitoring file behaviors.

8.3.18 Content Audit Alarming

The content audit alarming function is to send an alarming mail to the user containing content audit records.

Working Principle

Collect content audit records periodically and sent a mail to the user.

Related Configuraiton

Enabling Content Audit Alarming

Content audit alarming is disabled by default

8.3.19 Content Audti Reporting

The content audit reporting function is to collect content audit records in a report.

Working Principle

Creating a report periodically or automatically based in the report rule configured by the user.

Related Configuraiton

Configuring a Report Creation Time

No report creation time is configured by default.

8.4 Configuration

Configuration	Description and Command	
Configuring URL Classes	(Optional) It is used for reference by a URL object.	
	url class	Configures URL classes.
	url	Adds URL entries.
	comment	Configures descriptions.

Configuring URL Objects	(Mandatory) It is used for reference by a URL rule.	
	url-object	Configures URL objects.
	class	Adds URL classes.
	regexp	Adds regular expressions.
	comment	Configures descriptions.
Configuring Content Objects	(Mandatory) It is used for reference by a content audit rule.	
	content-object	Configures content objects.
	keyword	Adds keywords.
	regexp	Adds regular expressions.
	comment	Configures descriptions.
Configuring Policy Groups	(Mandatory) It is used to establish user-based behavior management.	
	content-policy	Configures policy groups.
	content-policy-config	Configures policy group attributes.
	content-policy-relate	Associates a policy group with a user.
Configuring Application Control Audit Rules	(Mandatory) It is used to create an application control audit policy.	
	app-rule	Configures application control audit rules.
	app-audit	Configures application control audit optimization.
Configuring URL Rules	(Mandatory) It is used to create a URL audit policy.	
	url-rule	Configures URL audit rules.
	url-audit	Configures URL audit optimization.
Enabling/Disabling Writing of Content Audit Information into the Local Memory	(Optional) It is used to determine whether to write the content audit information of each service into the local memory.	
	content-audit write-db {url | web-search | web-bbs | web-mail | mail | im | app-control | vid }	Enables/Disables writing of content audit information into the local memory.
Configuring HTTP Ports	(Optional) It is used to allow URL audit for flows via the HTTP ports except TCP port 80 and port 8080 when application identification is disabled.	
	content-audit http-port *port-num*	Configures HTTP ports.

Configuring HTTPS Ports	(Optional) It is used to allow domain name audit for flows via the HTTPS ports except TCP port 443 when application identification is disabled.	
	content-audit https-port *port-num*	Configures HTTPS ports.
Enabling/Disabling HTTPS Audit	(Optional) It is used to determine whether to audit and filter data flows of the HTTPS websites.	
	https-audit enable	Enables/Disables HTTPS audit.

8.4.1 Configuring URL Classes

Configuration Effect

Configure user-defined URL classes and URL entries contained therein.

Edit URL entries contained in system URL classes.

Display a URL system class or user-defined class to which a specific URL belongs.

Configure URL classes for reference by URL objects.

Notes

A URL class is validated only after it is referenced by a URL object.

Configuration Steps

Configuring URL Classes

Mandatory.

Configuring URL Entries

Optional. This function is configured to add or edit URL entries.

Configuring Descriptions

Optional. This function is configured to add descriptions of URL classes.

Verification

Display system URL classes.

Display user-defined URL classes.

Display a designated URL class.

Related Commands

Configuring URL Classes

Command	**url-class** *class-name*
Parameter Description	*class-name*: Specifies a name of a URL class.
Command Mode	Global configuration mode

Usage Guide	Generate a URL class and enter the URL class configuration mode. Run the **no** form of this command in global configuration mode to delete a URL class: **no url-class class-name**.

Configuring URL Entries

Command	**url** *url-string*
Parameter Description	*url-string*: Specifies URL entries contained in a URL class, with mode matching supported. 1. If a URL contained in a user-defined website class is a sub directory under the domain name, match all files under the sub directory. For example, if the URL is **ietf.org/2006**, match all content in the **ietf.org/2006** directory. 2. If a URL contained in a user-defined website class is a domain name and does not include a path, match all access to the domain name and its sub domain name. For example, if the URL is **ietf.org**, match access to sub domains including **www.ieft.org**, **download.ietf.org**, and **news.ietf.org**.
Command Mode	URL class configuration mode
Usage Guide	Use this command to add a URL entry to a URL class. Use the **no** form of this command to delete a URL entry: **no url** *url-string*.

Configuring Descriptions

Command	**comment** *comment-string*
Parameter Description	*comment-string*: Specifies a description of a URL class, and supports a maximum of 100 characters.
Command Mode	URL class configuration mode
Usage Guide	Use this command to describe usage of a URL class. Use the **no** form of this command to delete a description of a URL class: **no comment**.

Displaying Names of Classes in the URL Library of the System

Command	**show url-class system** [**class** { **id** *class-id* | **name** *class-name* }]
Parameter Description	*class-name*: Specifies a name of a designated system class. Information about all system URL classes is displayed if no class is designated. *class-id*: Specifies an ID of a designated system class.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to display classes in a system URL library.

Displaying Description Information About the System URL Library

Command	**show url-class system comment** [**class** { **id** *class-id* | **name** *class-name* }]
Parameter Description	*class-name*: Specifies a name of a designated system class. Information about all system URL classes is displayed if no class is designated.

	class-id: Specifies an ID of a designated system class.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to display description information about a system URL library.

Displaying Current User-defined Information of the URL Library of the System.

Command	**show url-class system custom** [**class** { **id** *class-id* | **name** *class-name* }]
Parameter Description	*class-name*: Specifies a name of a designated system class. Information about all system URL classes is displayed if no class is designated. *class-id*: Specifies an ID of a designated system class.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to display current user-defined information about a system URL library.

Displaying Related Information About the Exact Filtering Library

Command	**show url-class system exact**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to display related information about an exact filtering library.

Displaying URL Classes

Command	**show url-class url** *url-string*
Parameter Description	*url-string*: Specifies a string representing a URL.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to display a system URL class to which a designated URL string belongs, and the currently configured URL class.

Displaying Configuration Information of User-defined URL Classes

Command	**show url-class user-cfg** [*class-name*]
Parameter Description	*class-name*: Specifies a name of a user-defined class.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to display configuration information of a user-defined URL class.

Configuration Examples

Configuring User-defined URL Classes

Configuration Steps	● Configure the class CLASSA. ● Configure a URL entry to match all URLs of the sub domain name **ietf.org**. ● Configure the description **NEW-CLASSA**.
	FS# configure terminal FS(config)# url-class CLASSA FS(url-cls-config)# url ietf.org FS(url-cls-config)# comment NEW-CLASSA FS(url-cls-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

	FS# show running-config
	……
	url-class CLASSA
	  url ietf.org
	  comment NEW-CLASSA
	!……

Editing System URL Classes

Configuration Steps	● Enable the system class search engine. ● Add the URL entry **ietf.org**.
	FS# configure terminal FS(config)# url-class search engine FS(url-cls-config)# url ietf.org FS(url-cls-config)# end
Verification	● Run the **show running-config** command to display the configuration status.
	FS# show running-config …… url-class search engine url ietf.org

	!……

Displaying a System URL Class to Which a Designated URL String Belongs, and the Currently Configured URL Class

Configuration Steps	● Display class information of the URL **FS.com.cn**.
	FS# show url-class user-cfg CLASSA url-class:CLASSA url:ietf.org comment:comment for CLASSA
Verification	Display command output.

Common Errors

A regular expression does not meet a syntax requirement.

8.4.2 Configuring URL Objects

Configuration Effect

Create a URL object for reference by URL rules.

Notes

A URL object is validated only after it is referenced by a URL rule.

Configuration Steps

Configuring URL Objects

Mandatory.

Configuring URL Classes

Optional. This function is configured to add URL classes.

Configuring Regular Expressions

Optional. This function is configured to add regular expressions.

Configuring Descriptions

Optional. This function is configured to add descriptions of URL objects.

Verification

Run the show running-config command to display the configuration status.

Related Commands

Configuring URL Objects

Command	**url-object** *object-name*
Parameter Description	*object-name*: Specifies a name of a URL object.
Command Mode	Global configuration mode
Usage Guide	Generate a URL object and enter the URL object configuration mode. Run the **no** form of this command in global configuration mode to delete a URL object and all content contained therein: **no url-object** *object-name*.

Configuring URL Classes

Command	**class** *class-name*
Parameter Description	*class-name*: Specifies a name of a user-defined URL class or a URL class come with the system,
Command Mode	URL object configuration mode
Usage Guide	Add a keyword to a URL object. Use the **no** form of this command to delete a URL class: **no class** *class-name*.

Configuring Regular Expressions

Command	**regexp** *url-regexp*
Parameter Description	*url-regexp*: Specifies a URL regular expression, and supports a standard regular expression.
Command Mode	URL object configuration mode
Usage Guide	Add a URL regular expression to a URL object. Use the **no** form of this command to delete a regular expression: **no regexp** *url-regexp*.

Configuring Descriptions

Command	**comment** *comment-string*
Parameter Description	*comment-string*: Specifies a description of a URL object, and supports a maximum of 100 characters.
Command Mode	URL object configuration mode
Usage Guide	Use this command to describe usage of a URL object. Use the **no** form of this command to delete a description of a URL object: **no comment**.

Configuration Examples

Configuring Audit-free URL Objects

Configuration Steps	● Configure the URL object **un_audit_object**. ● Configure URL classes **un_audit_class**, **software update**, **script unknown**, and **software upgrade**. ● Configure the description **un_audit**.
	FS# configure terminal FS(config)# url-object objA FS(url-obj-config)# class un_audit_class FS(url-obj-config)# class software update FS(url-obj-config)# class script unknown FS(url-obj-config)# class software upgrade FS(url-obj-config)# comment un_audit FS(url-obj-config)# end
Verification	● Run the **show running-config** command to display the configuration status.
	FS# show running-config …… url-object un_audit_object class un_audit_class class software update class script unknown class software upgrade comment un_audit !……

Configuring URL Objects for File Blocking

Configuration Steps	● Configure the URL object **file_deny**. ● Configure a regular expression.

	FS# configure terminal
	FS(config)# url-object file_deny
	FS(url-obj-config)# regexp (\.exe$)\|(\.bat$)|(\.rmvb$)
	FS(url-obj-config)# end

Verification	● Run the **show running-config** command to display the configuration status.
	FS# show running-config …… url-object file_deny regexp (\.exe$)\|(\.bat$)|(\.rmvb$) !……

Common Errors

A regular expression does not meet a syntax requirement.

8.4.3 Configuring Content Objects

Configuration Effect

Create content objects for reference by content audit rules.

Notes

A content object is validated only after it is referenced by a URL rule.

Configuration Steps

Configuring Content Objects

Mandatory.

Configuring Keywords

Optional. Keywords can be added if any.

Configuring Regular Expressions

Optional. This function is configured to add regular expressions.

Configuring Descriptions

Optional. This function is configured to add descriptions of content objects.

Verification

Run the show running-config command to display the configuration status.

Related Commands

Configuring Content Objects

Command	**content-object** *object-name*
Parameter Description	*object-name*: Specifies a name of a content object.

Command Mode	Global configuration mode
Usage Guide	Use this command to generate a content object and enter the content object configuration mode. Use the **no** form of this command in global configuration mode to delete a content object and the information carried: **no content-object** *object-name*.

Configuring Keywords

Command	**keyword** *string*
Parameter Description	*string*: Specifies a keyword carried in a content object.
Command Mode	Content object configuration mode
Usage Guide	Use this command to add a keyword to a content object. Use the **no** form of this command to delete a keyword: **no keyword** *string*.

Configuring Regular Expressions

Command	**regexp** *regexp*
Parameter Description	*regexp*: Specifies a keyword regular expression, and supports a standard regular expression.
Command Mode	Content object configuration mode
Usage Guide	Use this command to add a keyword regular expression to a content object. Use the **no** form of this command to delete a regular expression: **no regexp** *regexp*.

Configuring Descriptions

Command	**comment** *comment-string*
Parameter Description	*comment-string*: Specifies a description of a content object, and supports a maximum of 100 characters.
Command Mode	Content object configuration mode
Usage Guide	Use this command to describe usage of a content object. Use the **no** form of this command to delete a description of a content object: **no comment**.

Configuration Examples

Configuring Content Objects

Configuration	● Configure the content object objA.

Steps	● Configure the keyword hello. ● Configure the regular match **.ietf.org**. ● Configure the description **commentA**.
	FS# configure terminal FS(config)# content-object objA FS(content-obj-config)# keyword hello FS(content-obj-config)# regexp .*\.ietf\.org FS(content-obj-config)# comment commentA FS(content-obj-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

	FS# show running-config
	……
	content-object objA
	  keyword hello
	  regexp .*\.ietf\.org
	  comment commentA
	!
	……

Common Errors

A regular expression does not meet a syntax requirement.

8.4.4 Configuring Policy Groups

Configuration Effect

Create policy groups.
Configure policy group attributes.
Associate a policy group with a user.

Notes

A policy group is validated only after it is associated with a valid user.
Compare priorities of policy groups first and then priorities of rules in the policy groups for policy matching.
A priority of an authenticated user is higher than that of a static user during policy matching.

Configuration Steps

Configuring Policy Groups

Mandatory.

Configuring Policy Group Attributes

Optional. Configure this function to edit policy group attributes.

Associating a Policy Group with a User

Mandatory.

Verification

Run the show running-config command to display the configuration status.

Related Commands

Configuring Policy Groups

Command	**content-policy** *policy-name*
Parameter Description	*policy-name*: Specifies a name of a content audit policy group.
Command Mode	Global configuration mode
Usage Guide	Specify a name of a content audit policy group, and enter the content audit policy group configuration mode. One policy group supports 100 members at most. Run the **no** form of this command in global configuration mode to delete a policy group and all content contained therein: **no content-policy** *policy-name*.

Disabling All Policy Groups

Command	**content-policy-config disable-all**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	1. Global disabling is valid only to user-defined policy groups and is invalid to system policy groups. 2. Use the **no** form of this command to cancel the global disabling function: **no content-policy-config disable-all**.

Disabling Policy Groups

Command	**content-policy-config disable-policy** *policy-name*
Parameter Description	*policy-name*: Specifies a name of a content audit policy group.
Command Mode	Global configuration mode
Usage Guide	1. Policy groups are valid by default. The policy group disabling command allows reserving a policy group configuration. However, such a policy group manner is not applied. Configure a disabling command explicitly to

	disable a certain policy group. 2. Running the policy group disabling command will not delete the association between policy group content and a user. 3. When the policy group disabling command is configured, this command is invalid when a specified policy group name does not exist. 4. After a policy group is deleted, a configuration for disabling the policy group will also be deleted at the same time. 5. Use the **no** form of this command to cancel policy disabling: **no content-policy-config disable-policy** *policy-name*.

Swapping Priorities of Policy Groups

Command	**content-policy-config priority-swap** *policy-name1 policy-name2*
Parameter Description	*policy-name1*: Specifies a name of one policy group that requires a priority swap. *policy-name2*: Specifies a name of the other policy group that requires a priority swap.
Command Mode	Global configuration mode
Usage Guide	After performing a configuration for swapping priorities of two policy groups, run the **show running** command to display a change in priority ranks of the two policy groups. Output of the **show running** command does not display the priority swap command.

Associating a Policy Group with a User

Command	**content-policy-relate relate** { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } } **policy** *policy-name*
Parameter Description	*subs-name1*: Specifies a static user associated with a policy group. *subs-name2*: Specifies an authenticated user associated with a policy group. *policy-name*: Specifies a name of a policy group.
Command Mode	Global configuration mode
Usage Guide	1. During rule association, if a policy group name does not exist, the association operation is invalid and this command does not exist. 2. During rule association, the associated users subs-name1 and subs-name2 may not exist. In this case, this command may exist but the rule is invalid. 3. During rule association, multiple user names can be specified for a static user or an authenticated user. The user names are separated by a comma, indicating that multiple users are associated with the policy group. The **policy-name** parameter allows for multiple policy groups, and the policy group names are separated by a comma. 4. Use the **no** form of this command to disable an association: **no content-policy-relate relate** { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } } **policy** *policy-name*.

Abandoning Inheritance of Policies of a Parent Subscriber Group

Command	**content-policy-relate no-inherit** { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } }
Parameter	*subs-name1*: Specifies a static user associated with a policy group.

Description	*subs-name2*: Specifies an authenticated user associated with a policy group.
Command Mode	Global configuration mode
Usage Guide	During configuration of the policy inheritance attribute of a user, the specified users subs-name1 and subs-name2 may not exist. If a policy is associated, this command exists but the rule is invalid. After the association between a user and all policy groups are deleted, the policy inheritance disabling attribute of the user will also be deleted. 2. Use the **no** form of this command to restore the policy inheritance attribute of the user: **no content-policy-relate no-inherit** { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } }.

Configuration Examples

Configuring Policy Groups

Configuration Steps	● Configure the content audit policy group policyA.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Configuring Policy Group Attributes

Configuration Steps	● Disable all user-defined policy groups.
	FS# configure terminal FS(config)# content-policy-config disable-all FS(config)# end
	● Disable the content audit policy group policyA.
	FS# configure terminal FS(config)# content-policy-config disable-policy policyA FS(config)# end
	● Swap priorities of the policy groups policyA and policyB.
	FS# configure terminal FS(config)# content-policy-config policy-swap policyA policyB

	FS(config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Common Errors

An actual audit result is different from expectation because priority relations between policies are not cleared.

8.4.5 Configuring Application Control Audit Rules

Configuration Effect

Add an application control audit rule to a content audit policy group.
Swap priorities of application control audit rules.
Configure application control audit optimization.

Notes

The validity status of an application control audit rule is subject to whether a referenced application class exists, whether a time object is valid, and whether a policy group to which the application control audit rule belongs is associated with a valid user.
In one policy group, a rule configured later has a higher priority.
No default application control audit rule is configured.
When the blocking rule of the application control audit function conflicts with the rules of other audit services, the application control audit has the highest priority. The data flows blocked by the application control audit function are free from other content audits.

Configuration Steps

Configuring Application Control Audit Rules

Mandatory.

Swapping Priorities of Application Control Audit Rules

Optional. This function is configured to swap priorities of application control audit rules.

Configuring Application Control Audit Optimization

Optional. This function is configured to change the default settings.

Verification

Run the show running-config command to display the configuration status.

Related Commands

Configuring Application Control Audit Rules

Command	**app-rule** *rule-id* **time-range** *time-name* **app-group** *app-group-name* **action** { **permit** | **deny** } [**audit**] [**vpn**] [**vip**] [**comment** *comment-string*]
Parameter	*rule-id*: Specifies the ID of a rule. A value range is **1** to **200**, and a maximum of 200 rules are supported.

Description	*app-group-name*: Specifies the name of an application group to be controlled by the rule. *time-name*: Specifies the name of a time object in a rule validity period. *comment-string*: Specifies the description of a rule.
Command Mode	Content audit policy group configuration mode
Usage Guide	1. The ID of a rule must be unique in one content audit policy group, and can be repeated in another content audit policy group. 2. All access control rules in a content audit policy group are prioritized, and the last configured rule has the highest priority. 3. A rule is invalid when the time name or application group name associated with the rule does not exist. 4. Use the **no** form of this command to delete an application control audit rule: **no app-rule** *rule-id*.

Deleting All Application Control Audit Rules in a Policy Group

Command	**app-rule delete-all**
Parameter Description	N/A
Command Mode	Content audit policy group configuration mode
Usage Guide	Use this command to delete all application control audit rules of the current policy group, without affecting other policy groups.

Swapping Priorities of Application Control Audit Rules

Command	**app-rule priority-swap** *rule-id1 rule-id2*
Parameter Description	*rule-id1*: Specifies the ID of rule 1 of which the priority is to be swapped. *rule-id2*: Specifies the ID of rule 2 of which the priority is to be swapped.
Command Mode	Content audit policy group configuration mode
Usage Guide	This priority swap command is used to swap priorities of two access control rules. After this command is run, run the **show running** command to display a change in ranks of the two rules. Output of the **show running** command does not display the priority swap command.

Configuring Application Control Audit Optimization

Command	**app-audit** { **optimize-cache** [*time*] | **optimize-deny** }
Parameter Description	*time*: Specifies a time period in a unit of seconds. After this function is enabled, the same application blocking action of one IP address is not repeatedly audited within this time period.

Command Mode	Global configuration mode
Usage Guide	1. After this function is enabled, the same application blocking action of one IP address is not repeatedly audited within this time period. The time period is 300s by default and ranges from 5s to 1800s. 2. There are two manners for blocking TCP flows: directly discard packets; and send RST packets to interrupt the connection. These two manners can be swapped via the configuration for optimizing application blocking. 3. This function is enabled by default. Use the **no** form of this command to disable the corresponding application control audit optimization function: **no no app-audit** { **optimize-cache** | **optimize-deny** }.

Configuration Example

Configuring Application Control Audit Rules

Configuration Steps	● Add an application control audit rule to the policy group policyA. Do not allow users to play videos or perform P2P download. Audit the corresponding filtering information.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# app-rule 2 time-range any direction double app-group VideoAndP2PGroup action deny audit comment DenyVideoAndP2P FS(cont-plcy-config)# end
	● Delete all application control audit rules in the policy group policyA.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# app-rule delete-all FS(cont-plcy-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Swapping Priorities of Application Control Audit Rules

Configuration Steps	● Swap priorities of the application control audit access control rules 10 and 20 in the policy group policyA.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# app-rule priority-swap 10 20

	FS(cont-plcy-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Configuring Application Control Audit Optimization

Configuration Steps	● Set the time period in which the repeated application blocking of one IP address is not audited to 120s.
	FS# configure terminal FS(config)# app-audit optimize-cache 120 FS(config)# end
	● Disable the application control audit optimization blocking.
	FS# configure terminal FS(config)# no app-audit optimize-deny FS(config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Common Errors

A repeated rule ID causes a configuration failure.
A rule is invalid because an object referenced by the rule does not exist.
An actual audit result is different from expectation because rule priorities are not cleared.

8.4.6 Configuring URL Rules

Configuration Effect

Enable the URL default audit function.
Add a URL rule to a content audit policy group.
Swap priorities of URL rules.
Configure URL audit optimization.
Configure content to be displayed on a URL filtering prompt page.

Notes

The validity status of a URL rule is subject to whether a referenced URL object exists, whether a time object is valid, and whether a policy group to which the URL rule belongs is associated with a valid user.
In one policy group, a rule configured later has a higher priority.

Configuration Steps

Configuring URL Rules

Mandatory.

Configuring URL Default Audit

Optional. This function is configured to enable default audit.

Swapping Priorities of URL Rules

Optional. This function is configured to swap priorities of URL rules.

Configuring URL Audit Optimization

Optional. This function is configured to edit default settings.

Configuring Content to Be Displayed on a URL Filtering Prompt Page

Optional. This function is configured to edit default settings.

Verification

Run the show running-config command to display the configuration status.

Related Commands

Configuring URL Rules

Command	**url-rule** *rule-id* **url-object** *url-obj-name* **time-range** *time-name* **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]
Parameter Description	*rule-id*: Specifies the ID of a rule. A value range is **1** to **200**, and a maximum of 200 rules are supported. *url-obj-name*: Specifies a URL object associated with a rule. *time-name*: Specifies the name of a time object in a rule validity period. *comment-string*: Specifies a description of a rule.
Command Mode	Content audit policy group configuration mode
Usage Guide	1. The ID of a rule must be unique in one content audit policy group, and can be repeated in another content audit policy group. 2. All access control rules in a content audit policy group are prioritized, and the last matched rule has the highest priority. 3. A rule is invalid when the time name or URL object name associated with the rule does not exist. 4. Use the **no** form of this command to delete a URL rule: **no url-rule** *rule-id*.

Configuring URL Default Audit

Command	**url-rule audit-default-enable**
Parameter	N/A

Description	
Command Mode	Content audit policy group configuration mode
Usage Guide	1. The URL default audit function valid only to a default audit group with a policy group named **_AUDIT_DEFAULT**. This command is invalid to other policy groups. 2. Use the **no** form of this command to disable the URL default audit function: **no url-rule audit-default-enable**.

Deleting All URL Rules in a Policy Group

Command	**url-rule delete-all**
Parameter Description	N/A
Command Mode	Content audit policy group configuration mode
Usage Guide	Delete all URL rules of the current policy group, without affecting other policy groups.

Swapping Priorities of URL Rules

Command	**url-rule priority-swap** *rule-id1 rule-id2*
Parameter Description	*rule-id1*: Specifies the ID of rule 1 of which the priority is to be swapped. *rule-id2*: Specifies the ID of rule 2 of which the priority is to be swapped.
Command Mode	Content audit policy group configuration mode
Usage Guide	This priority swap command is used to swap priorities of two access control rules. After this command is run, run the **show running** command to display a change in ranks of the two rules. Output of the **show running** command does not display the priority swap command.

Configuring URL Audit Optimization

Command	**url-audit** { **apply-referer** | **exact-filter** | **except-postfix** | **except-regexp** [*regexp*] | **only-get** | **optimize-cache** [*time*] }
Parameter Description	*regexp*: Specifies a regular expression. After this function is enabled, a URL that matches this regular expression is not audited. *time*: Specifies time period in a unit of seconds. After this function is enabled, a URL and a webpage displayed via this URL are not repeatedly audited within this time period.
Command Mode	Global configuration mode
Usage Guide	1. If no regular expression is specified when the **url-audit except-regexp** command is run, set the regular expression to **.*=.*&.*=.*** by default. 2. If the **url-audit except-postfix** command is run, do not audit URLs with the following suffixes: CSS, JS, GIF, PNG, SWF, BMP, ICO, NG, DLL, JPG, XML, and INI. 3. Run the **url-audit optimize-cache** command, and set the time period to **30s** by default.

	4. Run the **url-audit apply-referer** command in combination with a URL audit filtering policy. After the configuration is finished, match the corresponding URL, and match the **referer** field with the rules. This command is invalid if the URL audit filtering rule is not enabled. 5. This function is enabled by default. Use the **no** form of this command to disable the corresponding URL audit optimization function: **no url-audit** { **apply-referer** | **exact-filter** | **except-postfix** | **except-regexp** [*regexp*] | **only-get** | **optimize-cache** [*time*] }.

Configuring Content to Be Displayed on a URL Filtering Prompt Page

Command	**url-filter-notice display** [*text*]
Parameter Description	*text*: Specifies information to be displayed on a URL filtering prompt page. Default information is displayed if this parameter is not specified.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure content to be displayed on a URL filtering prompt page. This function is enabled by default, and content to be displayed is as follows: "You are forbidden to visit the website, please contact webmaster!"

Configuration Examples

Configuring URL Rules

Configuration Steps	● Add a URL access audit rule to the content audit policy group policyA. Do not access a URL in the URL object **url-objA**. Audit access from such URLs.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# url-rule 2 url-object url-objA time-range any action deny audit FS(cont-plcy-config)# end
	● Delete all URL rules in the policy group policyA.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# url-rule delete-all FS(cont-plcy-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Configuring URL Default Audit

Configuration	● Enable the URL default audit function.

Steps	
	FS# configure terminal FS(config)# content-policy _AUDIT_DEFAULT FS(cont-plcy-config)# url-rule audit-default-enable FS(cont-plcy-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Swapping Priorities of URL Rules

Configuration Steps	● Swap priorities of the URL access control rule 10 and the URL access control rule 20 in the policy group policyA.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# url-rule priority-swap 10 20 FS(cont-plcy-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Configuring URL Audit Optimization

Configuration Steps	● Audit only an HTTP GET operation.
	FS# configure terminal FS(config)# url-audit only-get FS(config)#end
	● Quit auditing a URL that meets the default regular expression (**.*=.*&.*=.***):
	FS# configure terminal FS(config)# url-audit except-regexp FS(config)# end
	● Quit auditing a URL with a suffix of a picture:
	FS# configure terminal FS(config)# url-audit except-postfix

	FS(config)# end
	● Quit auditing repeated URL access from a same IP address and a webpage displayed via the URL in 60s.
	FS# configure terminal FS(config)# url-audit optimize-cache 60 FS(config)# end
	● Configure a URL rule first, and then enable the URL loose whitelist function.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# url-rule 2 url-object url-objA time-range any action permit audit FS(cont-plcy-config)# exit FS(config)#url-rule apply-referer FS(config)#end
Verification	● Run the **show running-config** command to display the configuration status.

Configuring Content to Be Displayed on a URL Filtering Prompt Page

Configuration Steps	● Configure information to be displayed on a URL filtering prompt page.
	FS# configure terminal FS(config)# url-filter-notice display "You are forbidden to visit the website, please contact webmaster!" FS(config)#end
Verification	● Run the **show running-config** command to display the configuration status.

Common Errors

A repeated rule ID causes a configuration failure.

A rule is invalid because an object referenced by the rule does not exist.

An actual audit result is different from expectation because rule priorities are not cleared.

8.4.7 Configuring URL Redirection Rules

Configuration Effect

Add a URL redirection rule to a content audit policy group.

Swap priorities of URL redirection rules.

Notes

The validity status of a URL redirection rule is subject to whether a referenced time object is valid, and whether a policy group to which the URL redirection rule belongs is associated with a valid user.
In one policy group, a rule configured later has a higher priority.

Configuration Steps

Configuring URL Redirection Rules

Mandatory.

Swapping Priorities of URL Redirection Rules

Optional. This function is configured to swap priorities of URL redirection rules.

Verification

Run the show running-config command to display the configuration status.

Related Commands

Configuring URL Redirection Rules

Command	**url-redirect-rule** *rule-id* **time-range** *time-name* **from** *url-1* **to** *url-2* [**comment** *comment-string*]
Parameter Description	*rule-id*: Specifies the ID of a rule. A value range is **1** to **200**, and a maximum of 200 rules are supported. *time-name*: Specifies the name of a time object in a rule validity period. *url-1*: indicates the URL address to be redirected. *url-2*: indicates the URL address that is redirected to. *comment-string*: Specifies the description of a rule.
Command Mode	Content audit policy group configuration mode
Usage Guide	1. The ID of a rule must be unique in one content audit policy group, and can be repeated in another content audit policy group. 2. All URL redirection rules in a content audit policy group are prioritized, and the last configured rule has the highest priority. 3. A rule is invalid when the time name associated with the rule does not exist. 4. Use the **no** form of this command to delete a URL redirection rule: **no url-redirect-rule** *rule-id*.

Deleting All URL Redirection Rules in a Policy Group

Command	**url-redirect-rule delete-all**
Parameter Description	N/A
Command	Content audit policy group configuration mode

Mode	
Usage Guide	Use this command to delete all URL redirection rules of the current policy group, without affecting other policy groups.

Swapping Priorities of URL Redirection Rules

Command	**url-redirect-rule priority-swap** *rule-id1 rule-id2*
Parameter Description	*rule-id1*: Specifies the ID of rule 1 of which the priority is to be swapped. *rule-id2*: Specifies the ID of rule 2 of which the priority is to be swapped.
Command Mode	Content audit policy group configuration mode
Usage Guide	This priority swap command is used to swap priorities of two access control rules. After this command is run, run the **show running** command to display a change in ranks of the two rules. Output of the **show running** command does not display the priority swap command.

Configuration Example

Configuring URL Redirection Rules

Configuration Steps	● Add a URL redirection rule to the content audit policy group policyA. Redirect the access from www.sina.com.cn to www.FS.com.cn.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# url-redirect-rule 2 time-range any from www.sina.com.cn to www.FS.com.cn comment sina-redirect FS(cont-plcy-config)# end
	● Delete all URL redirection rules in the policy group policyA.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# url-redirect-rule delete-all FS(cont-plcy-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Swapping Priorities of URL Redirection Rules

Configuration Steps	● Swap priorities of the URL redirection rules 10 and 20 in the policy group policyA.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# url-redirect-rule priority-swap 10 20 FS(cont-plcy-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Common Errors

A repeated rule ID causes a configuration failure.
A rule is invalid because an object referenced by the rule does not exist.

8.4.8 Configuring IM Rules

Configuration Effect

Enable the IM default audit function.
Add an IM rule to a content audit policy group.
Swap priorities of IM rules.

Notes

The validity status of an IM rule is subject to whether a referenced content object exists, whether a time object is valid, and whether a policy group to which the IM rule belongs is associated with a valid user.
In one policy group, a rule configured later has a higher priority.

Configuration Steps

Configuring IM Rules

Mandatory.

Configuring IM Default Audit

Optional. This function is configured to enable the IM default audit.

Swapping Priorities of IM Rules

Optional. This function is configured to swap priorities of IM rules.

Verification

Run the show running-config command to display the configuration status.

Related Commands

Configuring Common Part in an IM Rule

Command	**im-rule** *rule-id* **time-range** *time-name* **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]
Parameter Description	*rule-id*: Specifies the ID of a rule. A value range is **1** to **200**. *time-name*: Specifies the name of a time object in a rule validity period. *comment-string*: Specifies the description of a rule.
Command Mode	Content audit policy group configuration mode
Usage Guide	1. The ID of a rule must be unique in one content audit policy group, and can be repeated in another content audit policy group. 2. All access control rules in a content audit policy group are prioritized, and the last configured rule has the highest priority. 3. A rule is invalid when the time name or content object name associated with the rule does not exist. 4. Use the **no** form of this command to delete an IM rule: **no im-rule** *rule-id.*

Configuring Description of an IM Rule

Command	**im-rule** *rule-id* **im-type** *im-name* [**relation** { **and** | **or** } [**account** *content-object-name1*] [**message** *content-object-name2*]]
Parameter Description	*rule-id*: Specifies the ID of a rule. A value range is **1** to **200**, and a maximum of 200 rules are supported. *im-name*: specifies IM software to be audited. ***im-name*** is a specified string. For example, if the string is **qq**, it indicates that only the QQ software is audited. If the string is **qq,msn** or **msn,qq**, it indicates that only QQ and MSN are audited. *content-object-name1*: specifies an IM account. If this parameter does not exist, it indicates that ***content-object-name1*** does not need to be matched. *content-object-name2*: specifies a chat record. If this parameter does not exist, it indicates that ***content-object-name2*** does not need to be matched.
Command Mode	Content audit policy group configuration mode
Usage Guide	QQ chat records are encrypted. At present, content filtering audit is not supported. (If the ***im-name*** value is **QQ**, the **message** parameter cannot be configured.)

Configuring IM Default Audit

Command	**im-rule audit-default-enable**
Parameter Description	N/A
Command Mode	Content audit policy group configuration mode

Usage Guide	1. The default audit function is valid only to a default audit group named **_AUDIT_DEFAULT**. This command is invalid to other policy groups. 2. Use the **no** form of this command to disable the IM default audit function: **no im-rule audit-default-enable**.

Deleting All IM Rules in a Policy Group

Command	**im-rule delete-all**
Parameter Description	N/A
Command Mode	Content audit policy group configuration mode
Usage Guide	Use this command to delete all IM rules of the current policy group, without affecting other policy groups.

Swapping Priorities of IM Rules

Command	**im-rule priority-swap** *rule-id1 rule-id2*
Parameter Description	*rule-id1*: Specifies the ID of rule 1 of which the priority is to be swapped. *rule-id2*: Specifies the ID of rule 2 of which the priority is to be swapped.
Command Mode	Content audit policy group configuration mode
Usage Guide	This priority swap command is used to swap priorities of two access control rules. After this command is run, run the **show running** command to display a change in ranks of the two rules. Output of the **show running** command does not display the priority swap command.

Configuration Example

Configuring IM Rules

Configuration Steps	● Add an MSN access audit rule to the content audit policy group policyA. Allow a user to use the MSN software for chatting. Audit a specific account accountA of this user or audit the chat record with a specific keyword keyA.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# im-rule 2 time-range any action permit audit comment PermitUserAMSN FS(cont-plcy-config)# im-rule 2 im-type msn relation or account accountA message keyA FS(cont-plcy-config)# end
	● Delete all IM rules in the policy group policyA.

	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# im-rule delete-all FS(cont-plcy-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Configuring IM Default Audit

Configuration Steps	● Enable the IM default audit function.
	FS# configure terminal FS(config)# content-policy _AUDIT_DEFAULT FS(cont-plcy-config)# im-rule audit-default-enable FS(cont-plcy-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Swapping Priorities of IM Rules

Configuration Steps	● Swap priorities of IM access control rules 10 and 20 in the policy group policyA.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# im-rule priority-swap 10 20 FS(cont-plcy-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Common Errors

A repeated rule ID causes a configuration failure.

If the description of a rule is configured without configuring the common part of the rule, a configuration failure is caused.

A rule is invalid because an object referenced by the rule does not exist.

An actual audit result is different from expectation because rule priorities are not cleared.

8.4.9 Configuring Mail Rules

Configuration Effect

Enable the mail default audit function.
Add a mail rule to a content audit policy group.
Swap priorities of mail rules.

Notes

The validity status of a mail rule is subject to whether a referenced content object exists, whether a time object is valid, and whether a policy group to which the mail rule belongs is associated with a valid user.
In one policy group, a rule configured later has a higher priority.

Configuration Steps

Configuring Mail Rules

Mandatory.

Configuring Mail Default Audit

Optional. This function is configured to enable the mail default audit.

Swap Priorities of Mail Rules

Optional. This function is configured to swap priorities of mail rules.

Verification

Run the show running-config command to display the configuration status.

Related Commands

Configuring Common Part in a Mail Rule

Command	**mail-rule** *rule-id* **time-range** *time-name* [**direction** { **in** | **out** | **double** }] **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]
Parameter Description	*rule-id*: Specifies the ID of a rule. A value range is **1** to **200**, and a maximum of 200 rules are supported. *time-name*: Specifies the name of a time object in a rule validity period. *comment-string*: Specifies the description of a rule.
Command Mode	Content audit policy group configuration mode
Usage Guide	1. The ID of a rule must be unique in one content audit policy group, and can be repeated in another content audit policy group. 2. All access control rules in a content audit policy group are prioritized, and the last configured rule has the highest priority. 3. A rule is invalid when the time name or content object name associated with the rule does not exist.

	4. Use the **no** form of this command to delete a mail rule: **no mail-rule** *rule-id.*

Configuring Description of a Mail Rule

Command	**mail-rule** *rule-id* **relation** { **and** | **or** } [**from** *content-object-name1*] [**to** *content-object-name2*] [**subject** *content-object-name3*] [**body** *content-object-name4*] [**attachment-name** *content-object-name5*] [**mail-size** { **greater** | **greater-equal** | **less** | **less-equal** } *file-size*]
Parameter Description	*rule-id*: Specifies the ID of a rule. A value range is **1** to **200**. *content-object-name1*: specifies a sender keyword. If this parameter does not exist, it indicates that ***content-object-name1*** does not need to be matched. *content-object-name2*: specifies a receiver keyword. If this parameter does not exist, it indicates that ***content-object-name2*** does not need to be matched. *content-object-name3*: specifies a mail title keyword. If this parameter does not exist, it indicates that ***content-object-name3*** does not need to be matched. *content-object-name4*: specifies a mail content keyword. If this parameter does not exist, it indicates that ***content-object-name4*** does not need to be matched. *content-object-name5*: specifies an attachment name keyword. If this parameter does not exist, it indicates that ***content-object-name5*** does not need to be matched. *file-size*: specifies the file size. It is an integer in the unit of KB.
Command Mode	Content audit policy group configuration mode
Usage Guide	1. When a rule is set to blocking, only the OR relation is valid. 2. A rule is invalid when the content object name associated with the rule does not exist.

Configuring Mail Default Audit

Command	**mail-rule audit-default-enable**
Parameter Description	N/A
Command Mode	Content audit policy group configuration mode
Usage Guide	1. The default audit function is valid only to a default audit group named **_AUDIT_DEFAULT**. This command is invalid to other policy groups. 2. Use the **no** form of this command to disable the mail default audit function: **no mail-rule audit-default-enable**.

Deleting All Mail Rules in a Policy Group

Command	**mail-rule delete-all**
Parameter Description	N/A

Command Mode	Content audit policy group configuration mode
Usage Guide	Use this command to delete all mail rules of the current policy group, without affecting other policy groups.

Swapping Priorities of Mail Rules

Command	**mail-rule priority-swap** *rule-id1 rule-id2*
Parameter Description	*rule-id1*: Specifies the ID of rule 1 of which the priority is to be swapped. *rule-id2*: Specifies the ID of rule 2 of which the priority is to be swapped.
Command Mode	Content audit policy group configuration mode
Usage Guide	This priority swap command is used to swap priorities of two access control rules. After this command is run, run the **show running** command to display a change in ranks of the two rules. Output of the **show running** command does not display the priority swap command.

Configuration Example

Configuring Mail Rules

Configuration Steps	● Add a mail access control rule to a content audit policy group policyA. Allow all users to send mails. Match the sender keyword OBJ-F or match the subject keyword OBJ-S or audit the mails smaller than 20,000 KB.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# mail-rule 1 time-range any action permit audit comment mail-audit-1 FS(cont-plcy-config)# mail-rule 1 relation or from OBJ-F subject OBJ-S mail-size less 20000 FS(cont-plcy-config)# end
	● Delete all mail rules in the policy group policyA.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# mail-rule delete-all FS(cont-plcy-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Configuring Mail Default Audit

Configuration Steps	● Enable the mail default audit function.
	FS# configure terminal FS(config)# content-policy _AUDIT_DEFAULT FS(cont-plcy-config)# mail-rule audit-default-enable FS(cont-plcy-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Swapping Priorities of Mail Rules

Configuration Steps	● Swap priorities of mail access control rules 10 and 20 in the policy group policyA.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# mail-rule priority-swap 10 20 FS(cont-plcy-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Common Errors

A repeated rule ID causes a configuration failure.

If the description of a rule is configured without configuring the common part of the rule, a configuration failure is caused.

A rule is invalid because an object referenced by the rule does not exist.

An actual audit result is different from expectation because rule priorities are not cleared.

8.4.10 Configuring Web BBS Rules

Configuration Effect

Enable the Web BBS default audit function.

Add a Web BBS rule to a content audit policy group.

Swap priorities of Web BBS rules.

Notes

The validity status of a Web BBS rule is subject to whether a referenced content object exists, whether a time object is valid, and whether a policy group to which the Web BBS rule belongs is associated with a valid user.

In one policy group, a rule configured later has a higher priority.

Configuration Steps

Configuring Web BBS Rules

Mandatory.

Configuring Web BBS Default Audit

Optional. This function is configured to enable the Web BBS default audit.

Swapping Priorities of Web BBS Rules

Optional. This function is configured to swap priorities of Web BBS rules.

Verification

Run the show running-config command to display the configuration status.

Related Commands

Configuring Web BBS Rules

Command	**web-bbs-rule** *rule-id* **time-range** *time-name* [**content** *content-object-name*] **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]
Parameter Description	*rule-id*: Specifies the ID of a rule. A value range is **1** to **200**, and a maximum of 200 rules are supported. *time-name*: Specifies the name of a time object in a rule validity period. *content-object-name*: Specifies the name of a content object used in a rule. *comment-string*: Specifies the description of a rule.
Command Mode	Content audit policy group configuration mode
Usage Guide	1. The ID of a rule must be unique in one content audit policy group, and can be repeated in another content audit policy group. 2. All access control rules in a content audit policy group are prioritized, and the last configured rule has the highest priority. 3. A rule is invalid when the time name or content object name associated with the rule does not exist. 4. Use the **no** form of this command to delete a Web BBS access control rule: **no web-bbs-rule** *rule-id*.

Configuring Web BBS Default Audit

Command	**web-bbs-rule audit-default-enable**
Parameter Description	N/A
Command Mode	Content audit policy group configuration mode

Usage Guide	1. The default audit function is valid only to a default audit group named **_AUDIT_DEFAULT**. This command is invalid to other policy groups. 2. Use the **no** form of this command to disable the Web BBS default audit function: **no web-bbs-rule audit-default-enable**.

Deleting All Web BBS Rules in a Policy Group

Command	**web-bbs-rule delete-all**
Parameter Description	N/A
Command Mode	Content audit policy group configuration mode
Usage Guide	Use this command to delete all Web BBS rules of the current policy group, without affecting other policy groups.

Swapping Priorities of Web BBS Rules

Command	**web-bbs-rule priority-swap** *rule-id1 rule-id2*
Parameter Description	*rule-id1*: Specifies the ID of rule 1 of which the priority is to be swapped. *rule-id2*: Specifies the ID of rule 2 of which the priority is to be swapped.
Command Mode	Content audit policy group configuration mode
Usage Guide	This priority swap command is used to swap priorities of two access control rules. After this command is run, run the **show running** command to display a change in ranks of the two rules. Output of the **show running** command does not display the priority swap command.

Configuration Example

Configuring Web BBS Rules

Configuration Steps	● Add a Web BBS rule to the content audit policy group policyA. Do not allow users to post messages with the specified keywords. Audit posted information.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# web-bbs-rule 2 time-range any content keyword-group action deny audit comment DenyInvalidBBS FS(cont-plcy-config)# end
	● Delete all Web BBS rules in the policy group policyA.

	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# web-bbs-rule delete-all FS(cont-plcy-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Configuring Web BBS Default Audit

Configuration Steps	● Enable the Web BBS default audit function.
	FS# configure terminal FS(config)# content-policy _AUDIT_DEFAULT FS(cont-plcy-config)# web-bbs-rule audit-default-enable FS(cont-plcy-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Swapping Priorities of Web BBS Rules

Configuration Steps	● Swap priorities of Web BBS access control rules 10 and 20 in the policy group policyA.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# web-bbs-rule priority-swap 10 20 FS(cont-plcy-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Common Errors

A repeated rule ID causes a configuration failure.

A rule is invalid because an object referenced by the rule does not exist.

An actual audit result is different from expectation because rule priorities are not cleared.

8.4.11 Configuring Web Mail Rules

Configuration Effect

Enable the Web mail default audit function.
Add a Web mail rule to a content audit policy group.
Swap priorities of Web mail rules.

Notes

The validity status of a Web mail rule is subject to whether a referenced content object exists, whether a time object is valid, and whether a policy group to which the Web mail rule belongs is associated with a valid user.
In one policy group, a rule configured later has a higher priority.

Configuration Steps

Configuring Web Mail Rules

Mandatory.

Configuring Web Mail Default Audit

Optional. This function is configured to enable the Web mail default audit.

Swapping Priorities of Web Mail Rules

Optional. This function is configured to swap priorities of Web mail rules.

Verification

Run the show running-config command to display the configuration status.

Related Commands

Configuring Common Part in a Web Mail Rule

Command	**web-mail-rule** *rule-id* **time-range** *time-name* [**direction** { **in** | **out** | **double** }] **action** { **permit** | **deny** } **audit** [**comment** *comment-string*]
Parameter Description	*rule-id*: Specifies the ID of a rule. A value range is **1** to **200**, and a maximum of 200 rules are supported. *time-name*: Specifies the name of a time object in a rule validity period. *comment-string*: Specifies the description of a rule.
Command Mode	Content audit policy group configuration mode
Usage Guide	1. The ID of a rule must be unique in one content audit policy group, and can be repeated in another content audit policy group. 2. All access control rules in a content audit policy group are prioritized, and the last configured rule has the highest priority. 3. A rule is invalid when the time name associated with the rule does not exist.

	4. Use the **no** form of this command to delete a Web mail rule: **no web-mail-rule** *rule-id.*

Configuring Description of a Web Mail Rule

Command	**web-mail-rule** *rule-id* **relation** { **and** | **or** } [**from** *content-object-name1*] [**to** *content-object-name2*] [**subject** *content-object-name3*] [**body** *content-object-name4*] [**attachment-name** *content-object-name5*]
Parameter Description	*rule-id*: Specifies the ID of a rule. A value range is **1** to **200**. *content-object-name1*: specifies a sender keyword. If this parameter does not exist, it indicates that ***content-object-name1*** does not need to be matched. *content-object-name2*: specifies a receiver keyword. If this parameter does not exist, it indicates that ***content-object-name2*** does not need to be matched. *content-object-name3*: specifies a mail title keyword. If this parameter does not exist, it indicates that ***content-object-name3*** does not need to be matched. *content-object-name4*: specifies a mail content keyword. If this parameter does not exist, it indicates that ***content-object-name4*** does not need to be matched. *content-object-name5*: specifies an attachment name keyword. If this parameter does not exist, it indicates that ***content-object-name5*** does not need to be matched.
Command Mode	Content audit policy group configuration mode
Usage Guide	1. When a rule is set to blocking, only the OR relation is valid. 2. A rule is invalid when the content object name associated with the rule does not exist.

Configuring Web Mail Default Audit

Command	**web-mail-rule audit-default-enable**
Parameter Description	N/A
Command Mode	Content audit policy group configuration mode
Usage Guide	1. The default audit function is valid only to a default audit group named **_AUDIT_DEFAULT**. This command is invalid to other policy groups. 2. Use the **no** form of this command to disable the Web mail default audit function: **no web-mail-rule audit-default-enable**.

Deleting All Web Mail Rules in a Policy Group

Command	**web-mail-rule delete-all**
Parameter Description	N/A

Command Mode	Content audit policy group configuration mode
Usage Guide	Use this command to delete all Web mail rules of the current policy group, without affecting other policy groups.

Swapping Priorities of Web Mail Rules

Command	**web-mail-rule priority-swap** *rule-id1 rule-id2*
Parameter Description	*rule-id1*: Specifies the ID of rule 1 of which the priority is to be swapped. *rule-id2*: Specifies the ID of rule 2 of which the priority is to be swapped.
Command Mode	Content audit policy group configuration mode
Usage Guide	This priority swap command is used to swap priorities of two access control rules. After this command is run, run the **show running** command to display a change in ranks of the two rules. Output of the **show running** command does not display the priority swap command.

Configuration Example

Configuring Web Mail Rules

Configuration Steps	● Add a Web mail access control rule to the content audit policy group policyA. Allow users to send a Web mail. Match the sender keyword OBJ-F or match the subject keyword OBJ-S.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# web-mail-rule 1 time-range any action permit audit comment mail-audit-1 FS(cont-plcy-config)# web-mail-rule 1 relation or from OBJ-F subject OBJ-S FS(cont-plcy-config)# end
	● Delete all Web mail rules in the policy group policyA.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# web-mail-rule delete-all FS(cont-plcy-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Configuring Web Mail Default Audit

Configuration Steps	● Enable the Web mail default audit function.
	FS# configure terminal FS(config)# content-policy _AUDIT_DEFAULT FS(cont-plcy-config)# web-mail-rule audit-default-enable FS(cont-plcy-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Swapping Priorities of Web Mail Rules

Configuration Steps	● Swap priorities of Web mail access control rules 10 and 20 in the policy group policyA.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# web-mail-rule priority-swap 10 20 FS(cont-plcy-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Common Errors

A repeated rule ID causes a configuration failure.

If the description of a rule is configured without configuring the common part of the rule, a configuration failure is caused.

A rule is invalid because an object referenced by the rule does not exist.

An actual audit result is different from expectation because rule priorities are not cleared.

8.4.12 Configuring Web Search Rules

Configuration Effect

Enable the Web search default audit function.

Add a Web search rule to a content audit policy group.

Swap priorities of Web search rules.

Notes

The validity status of a Web search rule is subject to whether a referenced content object exists, whether a time object is valid, and whether a policy group to which the Web search rule belongs is associated with a valid user.

In one policy group, a rule configured later has a higher priority.

Configuration Steps

Configuring Web Search Rules

Mandatory.

Configuring Web Search Default Audit

Optional. This function is configured to enable the Web search default audit.

Swapping Priorities of Web Search Rules

Optional. This function is configured to swap priorities of Web search rules.

Verification

Run the show running-config command to display the configuration status.

Related Commands

Configuring Web Search Rules

Command	**web-search-rule** *rule-id* **time-range** *time-name* [**content** *content-object-name*] **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*] **web-search-rule type** { **academic | book | dict | html | image | knows | map | music | news | others | shopping | social | stock | video**
Parameter Description	*rule-id*: Specifies the ID of a rule. A value range is **1** to **200**, and a maximum of 200 rules are supported. *time-name*: Specifies the name of a time object in a rule validity period. *content-object-name*: Specifies the name of a content object used in a rule. *comment-string*: Specifies the description of a rule. **Type**: Specifies the search type, e.g., image and map.
Command Mode	Content audit policy group configuration mode
Usage Guide	1. The ID of a rule must be unique in one content audit policy group, and can be repeated in another content audit policy group. 2. All access control rules in a content audit policy group are prioritized, and the last configured rule has the highest priority. 3. A rule is invalid when the time name or content object name associated with the rule does not exist. 4. Use the **no** form of this command to delete a Web search access control rule: **no web-search-rule** *rule-id*.

Configuring Web Search Default Audit

Command	**web-search-rule audit-default-enable**
Parameter	N/A

Description	
Command Mode	Content audit policy group configuration mode
Usage Guide	1. The default audit function is valid only to a default audit group named **_AUDIT_DEFAULT**. This command is invalid to other policy groups. 2. Use the **no** form of this command to disable the Web search default audit function: **no web-search-rule audit-default-enable**.

Deleting All Web Search Rules in a Policy Group

Command	**web-search-rule delete-all**
Parameter Description	N/A
Command Mode	Content audit policy group configuration mode
Usage Guide	Use this command to delete all Web search rules of the current policy group, without affecting other policy groups.

Swapping Priorities of Web Search Rules

Command	**web-search-rule priority-swap** *rule-id1 rule-id2*
Parameter Description	*rule-id1*: Specifies the ID of rule 1 of which the priority is to be swapped. *rule-id2*: Specifies the ID of rule 2 of which the priority is to be swapped.
Command Mode	Content audit policy group configuration mode
Usage Guide	This priority swap command is used to swap priorities of two access control rules. After this command is run, run the **show running** command to display a change in ranks of the two rules. Output of the **show running** command does not display the priority swap command.

Configuration Example

Configuring Web Search Rules

Configuration Steps	● Add a Web search access audit rule to the content audit policy group policyA. Filter the search that contains keyword-group, and audit the searched information.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# web-search-rule 2 time-range any content keyword-group action deny audit comment DenyInvalidSearch FS(cont-plcy-config)# end

	● Delete all Web search rules in the policy group policyA.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# web-search-rule delete-all FS(cont-plcy-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Configuring Web Search Default Audit

Configuration Steps	● Enable the Web search default audit function.
	FS# configure terminal FS(config)# content-policy _AUDIT_DEFAULT FS(cont-plcy-config)# web-search-rule audit-default-enable FS(cont-plcy-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Swapping Priorities of Web Search Rules

Configuration Steps	● Swap priorities of Web search access control rules 10 and 20 in the policy group policyA.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# web-search-rule priority-swap 10 20 FS(cont-plcy-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Common Errors

A repeated rule ID causes a configuration failure.

A rule is invalid because an object referenced by the rule does not exist.

An actual audit result is different from expectation because rule priorities are not cleared.

8.4.13 Configuring Virtual Identity Rules

Configuration Effect

Enable the virtual identity default audit function.

Notes

None.

Configuration Steps

Configuring Virtual Identity Default Audit

Mandatory. This function is configured to enable the virtual identity default audit.

Verification

Run the show running-config command to display the configuration status.

Related Commands

Configuring Virtual Identity Default Audit

Command	**vid-rule audit-default-enable**
Parameter Description	N/A
Command Mode	Content audit policy group configuration mode
Usage Guide	1. The default audit function is valid only to a default audit group named **_AUDIT_DEFAULT**. This command is invalid to other policy groups. 2. Use the **no** form of this command to disable the virtual identity default audit function: **no vid-rule audit-default-enable**.

Configuration Example

Configuring Virtual Identity Default Audit

Configuration Steps	● Enable the virtual identity default audit function.
	FS# configure terminal FS(config)# content-policy _AUDIT_DEFAULT FS(cont-plcy-config)# vid-rule audit-default-enable FS(cont-plcy-config)# end

Verification	● Run the **show running-config** command to display the configuration status.

Common Errors

N/A

8.4.14 Configuring QQ Chat Audit Rules

Configuration Effect

Enable the default QQ chat audit function.
Add a QQ chat audit rule, that is, plug-in-based audit rule, to a content audit policy group.
Swap priorities of plug-in-based audit rules.
Configure the method for downloading the plug-in to the client.

Notes

The validity status of a plug-in-based audit rule is subject to whether a referenced content object exists, whether a time object is valid, and whether a policy group to which the plug-in-based audit rule belongs is associated with a valid user.
In one policy group, a rule configured later has a higher priority.
For the same device, clients support only one download method.

Configuration Steps

Configuring Plug-in-based Audit Rules

Mandatory.

Configuring Plug-in-based Default Audit

Optional. This function is configured to enable the default plug-in-based audit.

Swapping Priorities of Plug-in-based Audit Rules

Optional. This function is configured to swap priorities of plug-in-based audit rules.

Configuring the Method for Downloading Plug-in to the Client

Optional. This function is configured to set the server, protocol, and port number for downloading the plug-in to the intranet client.

Verification

Run the show running-config command to display the configuration status.

Related Commands

Configuring Plug-in-based Audit Rules

Command	**plugin-rule** *rule-id* **time-range** *time-name* [**content** *content-object-name*] **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]

Parameter Description	*rule-id*: Specifies the ID of a rule. A value range is **1** to **200**, and a maximum of 200 rules are supported. *time-name*: Specifies the name of a time object in a rule validity period. *content-object-name*: Specifies the name of a content object used in a rule. *comment-string*: Specifies the description of a rule.
Command Mode	Content audit policy group configuration mode
Usage Guide	1. The ID of a rule must be unique in one content audit policy group, and can be repeated in another content audit policy group. 2. All access control rules in a content audit policy group are prioritized, and the last configured rule has the highest priority. 3. A rule is invalid when the time name or content object name associated with the rule does not exist. 4. Use the **no** form of this command to delete a plug-in-based access control rule: **no plugin-rule** *rule-id*.

Configuring Plug-in-based Default Audit

Command	**plugin-rule audit-default-enable**
Parameter Description	N/A
Command Mode	Content audit policy group configuration mode
Usage Guide	1. The default audit function is valid only to a default audit group named **_AUDIT_DEFAULT**. This command is invalid to other policy groups. 2. Use the **no** form of this command to disable the plug-in-based default audit function: **no plugin-rule audit-default-enable**.

Deleting All Plug-in-based Audit Rules in a Policy Group

Command	**plugin-rule delete-all**
Parameter Description	N/A
Command Mode	Content audit policy group configuration mode
Usage Guide	Use this command to delete all plug-in-based audit rules of the current policy group, without affecting other policy groups.

Swapping Priorities of Plug-in-based Audit Rules

Command	**plugin-rule priority-swap** *rule-id1 rule-id2*
Parameter Description	*rule-id1*: Specifies the ID of rule 1 of which the priority is to be swapped. *rule-id2*: Specifies the ID of rule 2 of which the priority is to be swapped.
Command Mode	Content audit policy group configuration mode
Usage Guide	This priority swap command is used to swap priorities of two access control rules. After this command is run, run the **show running** command to display a change in ranks of the two rules. Output of the **show running**

	command does not display the priority swap command.

Configuring a Protocol and Port Number for Downloading the Plug-in to the Client

Command	**plugin-config set-download-protol protol** *protolname* **port** *portnum*
Parameter Description	*protolname*: Specifies a protocol (only HTTP and HTTPS are supported) for downloading the plug-in from the device to the intranet client. *portnum*: Specifies a port number for downloading the plug-in from the device to the intranet client.
Command Mode	Global configuration mode
Usage Guide	After this command is run, run the **show running** command to display the protocol and port number for downloading the plug-in from the device to the intranet client.

Configuring a URL Address for Downloading the Plug-in to the Client

Command	**plugin-config set-download-url** *urlstring*
Parameter Description	*urlstring*: Specifies a URL address for downloading the plug-in to the intranet client.
Command Mode	Global configuration mode
Usage Guide	After this command is run, run the **show running** command to display the URL address for downloading the plug-in to the intranet client.

Configuration Example

Configuring Plug-in-based Audit Rules

Configuration Steps	Delete all plug-in-based audit rules in the policy group policyA.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# plugin-rule delete-all FS(cont-plcy-config)# end
Verification	Run the **show running-config** command to display the configuration status.

Configuring Plug-in-based Default Audit

Configuration Steps	Enable plug-in-based default audit.
	FS# configure terminal FS(config)# content-policy _AUDIT_DEFAULT FS(cont-plcy-config)# plugin-rule audit-default-enable FS(cont-plcy-config)# end
Verification	Run the **show running-config** command to display the configuration status.

Swapping Priorities of Plug-in-based Audit Rules

Configuration Steps	Swap priorities of plug-in-based access control rules 10 and 20 in the policy group policyA.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# plugin-rule priority-swap 10 20 FS(cont-plcy-config)# end
Verification	Run the **show running-config** command to display the configuration status.

Configuring a Blacklist

Configuration Steps	Configure a blacklist.
	FS# configure terminal FS(config)#content-policy _TOP_PRIORITY FS(cont-plcy-config) plugin-rule 1 time-range any action deny audit comment testcomment FS(cont-plcy-config)#end
Verification	Run the **show running-config** command to display the configuration status.

Configuring a Whitelist

Configuration Steps	Configure a whitelist.
	FS# configure terminal FS(config)#content-policy _AUDIT_DEFAULT FS(cont-plcy-config)#plugin-rule audit-default-enable FS(cont-plcy-config)#end FS# configure terminal FS(config)#content-policy _TOP_PRIORITY FS(cont-plcy-config) plugin-rule 1 time-range any action permit audit comment testcomment FS(cont-plcy-config)#end
Verification	Run the **show running-config** command to display the configuration status.

Configuring a Protocol and Port Number for Downloading the Plug-in

Configuration Steps	Configure HTTPS for downloading the plug-in from the device to the intranet client.
	FS# configure terminal FS(config)# plugin-config set-download-protol protol https port 4430 FS(cont-plcy-config)#end
Verification	Run the **show running-config** command to display the configuration status.

Configuring the Intranet Client to Download the Plug-in from the Intranet Server

Configuration Steps	Configure the intranet client to download the plug-in from the intranet server.

	FS# configure terminal FS(config)# plugin-config set-downloa-url http://192.168.1.10/download/ FS(cont-plcy-config)#end
Verification	Run the **show running-config** command to display the configuration status.

Common Errors

A repeated rule ID causes a configuration failure.

A rule is invalid because an object referenced by the rule does not exist.

An actual audit result is different from expectation because rule priorities are not cleared.

8.4.15 Configuring Posted File Audit Rules

Configuration Effect

Enable the posted file default audit function.

Add a posted file audit rule to a content audit policy group.

Swap priorities of posted file audit rules.

Notes

The validity status of a posted file audit rule is subject to whether a referenced content object exists, whether a time object is valid, and whether a policy group to which the posted file rule belongs is associated with a valid user.

In one policy group, a rule configured later has a higher priority.

Configuration Steps

Configuring Posted File Audit Rules

Mandatory.

Configuring Posted File Default Audit

Optional. This function is configured to enable the posted file default audit.

Swapping Priorities of Posted File Audit Rules

Optional. This function is configured to swap priorities of posted file audit rules.

Verification

Run the show running-config command to display the configuration status.

Related Commands

Configuring Posted File Audit Rules

Command	**postfile-rule** *rule-id* **time-range** *time-name* [**content** *content-object-name*] **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]

Parameter Description	*rule-id*: Specifies the ID of a rule. A value range is **1** to **200**, and a maximum of 200 rules are supported. *time-name*: Specifies the name of a time object in a rule validity period. *content-object-name*: Specifies the name of a content object used in a rule. *comment-string*: Specifies the description of a rule.
Command Mode	Content audit policy group configuration mode
Usage Guide	1. The ID of a rule must be unique in one content audit policy group, and can be repeated in another content audit policy group. 2. All access control rules in a content audit policy group are prioritized, and the last configured rule has the highest priority. 3. A rule is invalid when the time name or content object name associated with the rule does not exist. 4. Use the **no** form of this command to delete a posted file access control rule: **no postfile-rule** *rule-id*.

Configuring Posted File Default Audit

Command	**postfile-rule audit-default-enable**
Parameter Description	N/A
Command Mode	Content audit policy group configuration mode
Usage Guide	1. The default audit function is valid only to a default audit group named **_AUDIT_DEFAULT**. This command is invalid to other policy groups. 2. Use the **no** form of this command to disable the posted file default audit function: **no postfile-rule audit-default-enable**.

Deleting All Posted File Audit Rules in a Policy Group

Command	**postfile-rule delete-all**
Parameter Description	N/A
Command Mode	Content audit policy group configuration mode
Usage Guide	Use this command to delete all posted file audit rules of the current policy group, without affecting other policy groups.

Swapping Priorities of Posted File Audit Rules

Command	**postfile-rule priority-swap** *rule-id1 rule-id2*
Parameter Description	*rule-id1*: Specifies the ID of rule 1 of which the priority is to be swapped. *rule-id2*: Specifies the ID of rule 2 of which the priority is to be swapped.
Command Mode	Content audit policy group configuration mode
Usage Guide	This priority swap command is used to swap priorities of two access control rules. After this command is run, run the **show running** command to display a change in ranks of the two rules. Output of the **show running**

	command does not display the priority swap command.

Configuration Example

Configuring Posted File Audit Rules

Configuration Steps	Add a posted file audit rule to the content audit policy group policyA, to filter the posted files and audit the user behavior.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# postfile-rule 2 time-range any content keyword-group action deny audit comment TEST FS(cont-plcy-config)# end
	Delete all posted file audit rules in the policy group policyA.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# postfile-rule delete-all FS(cont-plcy-config)# end
Verification	Run the **show running-config** command to display the configuration status.

Configuring Posted File Default Audit

Configuration Steps	Enable posted file default audit.
	FS# configure terminal FS(config)# content-policy _AUDIT_DEFAULT FS(cont-plcy-config)# postfile-rule audit-default-enable FS(cont-plcy-config)# end
Verification	Run the **show running-config** command to display the configuration status.

Swapping Priorities of Posted File Audit Rules

Configuration Steps	Swap priorities of posted file access control rules 10 and 20 in the policy group policyA.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# postfile-rule priority-swap 10 20 FS(cont-plcy-config)# end
Verification	Run the **show running-config** command to display the configuration status.

Common Errors

A repeated rule ID causes a configuration failure.

A rule is invalid because an object referenced by the rule does not exist.

An actual audit result is different from expectation because rule priorities are not cleared.

8.4.16 Configuring HTTP Post Audit Rules

Configuration Effect

Enable the HTTP post default audit function.
Add an HTTP post audit rule, that is, a post audit rule, to a content audit policy group.
Swap priorities of post audit rules.

Notes

The validity status of a post audit rule is subject to whether a referenced content object exists, whether a time object is valid, and whether a policy group to which the post audit rule belongs is associated with a valid user.
In one policy group, a rule configured later has a higher priority.

Configuration Steps

Configuring Post Audit Rules

Mandatory.

Configuring Post Default Audit

Optional. This function is configured to enable the post default audit.

Swapping Priorities of Post Audit Rules

Optional. This function is configured to swap priorities of post audit rules.

Verification

Run the show running-config command to display the configuration status.

Related Commands

Configuring Post Audit Rules

Command	**post-rule** *rule-id* **time-range** *time-name* [**content** *content-object-name*] **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]
Parameter Description	*rule-id*: Specifies the ID of a rule. A value range is **1** to **200**, and a maximum of 200 rules are supported. *time-name*: Specifies the name of a time object in a rule validity period. *content-object-name*: Specifies the name of a content object used in a rule. *comment-string*: Specifies the description of a rule.
Command Mode	Content audit policy group configuration mode
Usage Guide	1. The ID of a rule must be unique in one content audit policy group, and can be repeated in another content audit policy group. 2. All access control rules in a content audit policy group are prioritized, and the last configured rule has the highest priority. 3. A rule is invalid when the time name or content object name associated with the rule does not exist. 4. Use the **no** form of this command to delete a post access control rule: **no post-rule** *rule-id*.

Configuring Post Default Audit

Command	**post-rule audit-default-enable**
Parameter Description	N/A
Command Mode	Content audit policy group configuration mode
Usage Guide	1. The default audit function is valid only to a default audit group named **_AUDIT_DEFAULT**. This command is invalid to other policy groups. 2. Use the **no** form of this command to disable the post default audit function: **no post-rule audit-default-enable**.

Deleting All Post Audit Rules in a Policy Group

Command	**post-rule delete-all**
Parameter Description	N/A
Command Mode	Content audit policy group configuration mode
Usage Guide	Use this command to delete all post audit rules of the current policy group, without affecting other policy groups.

Swapping Priorities of Post Audit Rules

Command	**post-rule priority-swap** *rule-id1 rule-id2*
Parameter Description	*rule-id1*: Specifies the ID of rule 1 of which the priority is to be swapped. *rule-id2*: Specifies the ID of rule 2 of which the priority is to be swapped.
Command Mode	Content audit policy group configuration mode
Usage Guide	This priority swap command is used to swap priorities of two access control rules. After this command is run, run the **show running** command to display a change in ranks of the two rules. Output of the **show running** command does not display the priority swap command.

Configuration Example

Configuring Post Audit Rules

Configuration Steps	Add a post audit rule to the content audit policy group policyA, to filter the posted information and audit the user behavior.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# post-rule 2 time-range any content keyword-group action deny audit comment TEST FS(cont-plcy-config)# end
	Delete all post audit rules in the policy group policyA.
	FS# configure terminal

	FS(config)# content-policy policyA FS(cont-plcy-config)# post-rule delete-all FS(cont-plcy-config)# end
Verification	Run the **show running-config** command to display the configuration status.

Configuring Post Default Audit

Configuration Steps	Enable post default audit.
	FS# configure terminal FS(config)# content-policy _AUDIT_DEFAULT FS(cont-plcy-config)# post-rule audit-default-enable FS(cont-plcy-config)# end
Verification	Run the **show running-config** command to display the configuration status.

Swapping Priorities of Post Audit Rules

Configuration Steps	Swap priorities of post access control rules 10 and 20 in the policy group policyA.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# post-rule priority-swap 10 20 FS(cont-plcy-config)# end
Verification	Run the **show running-config** command to display the configuration status.

Common Errors

A repeated rule ID causes a configuration failure.

A rule is invalid because an object referenced by the rule does not exist.

An actual audit result is different from expectation because rule priorities are not cleared.

8.4.17 Enabling Encryption-type Audit

Configuration Effect

Enable the encryption-type audit function.

Enable the encryption-type audit function for some users.

Disable the encryption-type audit function for some users.

Notes

The encryption-type audit function can only be enabled under the default audit policy and is a global function.

The encryption-type audit function cannot take effect independently and needs to be validated in combination with the audit policies of various applications such as Web BBS, Web mail, Web search, virtual identity, and posted file.

Configuration Steps

Enabling Encryption-type Audit

Mandatory.

Enabling Encryption-type Audit for Some Users

Optional.

Disabling Encryption-type Audit for Some Users

Optional.

Verification

Run the show running-config command to display the configuration status.

Related Commands

Enabling Encryption-type Audit

Command	**ssl-audit enable**
Parameter Description	N/A
Command Mode	Content audit default policy group configuration mode
Usage Guide	Use the **no** form of this command to disable the encryption-type audit function: **no ssl-audit enable**.

Enabling Encryption-type Audit for Some Users

Command	**ssl-audit need-proxy subscriber** *usr_group* **ssl-audit need-proxy auth-subscriber** *usr_group_auth*
Parameter Description	*usr_group*: Specifies a static user group. *usr_group_auth*: Specifies an authenticated user group.
Command Mode	Global configuration mode
Usage Guide	Run the **show ssl-audit need-proxy** command to display the configuration result.

Disabling Encryption-type Audit for Some Users

Command	**ssl-audit unneed-proxy subscriber** *usr_group* **ssl-audit unneed-proxy auth-subscriber** *usr_group_auth*
Parameter Description	*usr_group*: Specifies a static user group. *usr_group_auth*: Specifies an authenticated user group.
Command Mode	Global configuration mode
Usage Guide	Run the **show ssl-audit unneed-proxy** command to display the configuration result.

Configuration Example

Enabling Encryption-type Audit

Configuration Steps	Enable the encryption-type audit function.
	FS# configure terminal FS(config)# content-policy _AUDIT_DEFAULT FS(cont-plcy-config)# ssl-audit enable FS(cont-plcy-config)# end
	Disable the encryption-type audit function.
	FS# configure terminal FS(config)# content-policy _AUDIT_DEFAULT FS(cont-plcy-config)# no ssl-audit enable FS(cont-plcy-config)# end
Verification	Run the **show running-config** command to display the configuration status.

Enabling Encryption-type Audit for Some Users

Configuration Steps	Enable the encryption-type audit function for some users.
	FS# configure terminal FS(config)# ssl-audit need-proxy subscriber usr_group_sub FS(config)# ssl-audit need-proxy auth-subscriber usr_group_auth FS(cont-plcy-config)# end
	Cancel the encryption-type audit function enabled for some users.
	FS# configure terminal FS(config)# no ssl-audit need-proxy subscriber usr_group_sub FS(config)# no ssl-audit need-proxy auth-subscriber usr_group_auth FS(cont-plcy-config)# end
Verification	Run the **show ssl-audit unneed-proxy** command to display the configuration status.

Disabling Encryption-type Audit for Some Users

Configuration Steps	Disable the encryption-type audit function for some users.
	FS# configure terminal FS(config)# ssl-audit unneed-proxy subscriber usr_group_sub FS(config)# ssl-audit unneed-proxy auth-subscriber usr_group_auth FS(cont-plcy-config)# end
	Cancel the encryption-type audit function disabled for some users.
	FS# configure terminal FS(config)# no ssl-audit unneed-proxy subscriber usr_group_sub FS(config)# no ssl-audit unneed-proxy auth-subscriber usr_group_auth FS(cont-plcy-config)# end
Verification	Run the **show ssl-audit unneed-proxy** command to display the configuration status.

Common Errors

N/A

8.4.18 Configuring Blocked Information Real-time Statistics Collection

Configuration Effect

Set an IP address for statistics collection.

Notes

This function is a global function.
This function cannot take effect independently and needs to be validated in combination with the audit policies of various applications such as URL, IM, mail, Web BBS, Web mail, Web search, virtual identity, and posted file.
If an IP address is set, this function collects statistics of the blocked information of the IP address only.

Configuration Steps

Setting an IP Address for Statistics Collection

Optional.

Verification

Run the show running-config command to display the configuration status.

Related Commands

Setting an IP Address for Statistics Collection

Command	**content-audit deny-stat ip** { A.B.C.D | X:X:X:X::X }
Parameter Description	A.B.C.D: Specifies an IP address.
Command Mode	Privileged EXEC mode
Usage Guide	Use the **no** form of this command to cancel statistics collection of an IP address: **no content-audit deny-stat ip** { A.B.C.D | X:X:X:X::X }.

Configuration Example

Setting an IP Address for Statistics Collection

Configuration Steps	Set an IP address for statistics collection.
	FS# configure terminal FS(config)# content-audit deny-stat ip 192.168.1.2 FS(config)# end
	Cancel statistics collection of an IP address.
	FS# configure terminal

	FS(config)#no content-audit deny-stat ip 192.168.1.2 FS(config)# end
Verification	Run the **show running-config** command to display the configuration status.

Common Errors

N/A

8.4.19 Enabling/Disabling Writing of Content Audit Information into the Local Memory

Configuration Effect

By default, content audit information of each service is saved in the memory of the device. If audit information is sent to an external log server, disable saving of audit information to the local memory.

Notes

None.

Configuration Steps

Enabling/Disabling Writing of the Content Audit Information of Each Service into the Local Memory

Optional.

Verification

Run the show content-audit write-db/show running-config command to display the configuration status.

Related Commands

Enabling/Disabling Writing of URL Audit Information into the Local Memory

Command	**content-audit write-db url**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Run the **no content-audit write-db url** command to disable writing of URL audit information into the local memory.

Enabling/Disabling Writing of Web Search Audit Information into the Local Memory

Command	**content-audit write-db web-search**
Parameter Description	N/A
Command Mode	Global configuration mode

Usage Guide	Run the **no content-audit write-db web-search** command to disable writing of Web search audit information into the local memory.

Enabling/Disabling Writing of Web BBS Audit Information into the Local Memory

Command	**content-audit write-db web-bbs**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Run the **no content-audit write-db web-bbs** command to disable writing of Web BBS audit information into the local memory.

Enabling/Disabling Writing Web Mail Audit Information into the Local Memory

Command	**content-audit write-db web-mail**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Run the **no content-audit write-db web-mail** command to disable writing of Web mail audit information into the local memory.

Enabling/Disabling Writing of Mail Audit Information into the Local Memory

Command	**content-audit write-db mail**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Run the **no content-audit write-db mail** command to disable writing of mail audit information into the local memory.

Enabling/Disabling Writing of IM Audit Information into the Local Memory

Command	**content-audit write-db im**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Run the **no content-audit write-db im** command to disable writing of IM audit information into the local memory.

Enabling/Disabling Writing of Application Control Audit Information into the Local Memory

Command	**content-audit write-db app-control**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Run the **no content-audit write-db app-control** command to disable writing of application control audit information into the local memory.

Enabling/Disabling Writing of Virtual Identity Audit Information into the Local Memory

Command	**content-audit write-db vid**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Run the **no content-audit write-db vid** command to disable writing of virtual identity audit information into the local memory.

Configuration Example

Enabling Writing of Content Audit Information of Each Service into the Local Memory

Configuration Steps	● In global configuration mode, enable writing of audit information of each service into the local memory.
	FS# configure terminal FS(config)# content-audit write-db url FS(config)# content-audit write-db im FS(config)# content-audit write-db app-control FS(config)# content-audit write-db web-search FS(config)# content-audit write-db web-bbs FS(config)# content-audit write-db web-mail FS(config)# content-audit write-db mail FS(config)# content-audit write-db vid FS(config)# end
Verification	● Run the **show content-audit write-db** command to display the configuration status.

	FS# show content-audit write-db url_write_db: 1 im_write_db: 1 app_control_write_db: 1 web_search_write_db: 1 web_bbs_write_db: 1 web_mail_write_db: 1 mail_write_db: 1 vid_write_db: 1

Common Errors

N/A

8.4.20 Configuring HTTP Ports

Configuration Effect

When content audit does not rely on application identification, identify HTTP packets via ports. By default, identify HTTP packets via the TCP port 80 and port 8080. For other special HTTP packets, run this command to configure an HTTP to identify the HTTP packets.

Notes

A configured HTTP port is validated within 3 seconds.

Configuration Steps

Configuring HTTP Ports

Optional. By default, the TCP port 80 and port 8080 are used to identify HTTP packets in the system. Other ports can be added to identify other special HTTP packets.

Verification

Run the show content-audit http-port command to display the configuration status.

Related Commands

Configuring HTTP Ports

Command	**content-audit http-port** *port-num*
Parameter Description	*port-num*: Specifies a port number. A value range is **1** to **65535**. Port 80 and port 8080 are default system ports and are not allowed to manually add or delete.
Command Mode	Global configuration mode

Usage Guide	Add an HTTP port. Use the **no** form of this command to delete an HTTP port: **no content-audit http-port** *port-num*.

Configuration Examples

Adding an HTTP Port

Configuration Steps	● Add the HTTP port 60000.
	FS# configure terminal FS(config)# content-audit http-port 60000 FS(url-obj-config)# end
Verification	● Run the **show content-audit http-port** command to display the configuration status.
	FS#show content-audit http-port HTTP port information in user: 80 8080 60000 HTTP port information in kernel: 80 8080 60000

Deleting an HTTP Port

Configuration Steps	● Delete the HTTP port 60000.
	FS# configure terminal FS(config)# no content-audit http-port 60000 FS(url-obj-config)# end
Verification	● Run the **show content-audit http-port** command to display the configuration status.
	FS#show content-audit http-port HTTP port information in user: 80

	8080 HTTP port information in kernel: 80 8080

Common Errors

N/A

8.4.21 Configuring HTTPS Ports

Configuration Effect

When content audit does not rely on application identification, identify HTTPS packets via ports. By default, identify HTTPS packets via TCP Port 443. For other special HTTPS packets, run this command to configure an HTTPS port to identify the HTTPS packets.

Notes

A configured HTTPS port is validated within 3 seconds.

Configuration Steps

Configuring HTTPS Ports

Optional. By default, TCP Port 443 is used to identify HTTPS packets in the system. Other ports can be added to identify other special HTTPS packets.

Verification

Run the show content-audit https-port command to display the configuration status.

Related Commands

Configuring HTTPS Ports

Command	**content-audit https-port** *port-num*
Parameter Description	*port-num*: Specifies a port ID. A value range is **1** to **65535**. Port 443 is the default system port and is not allowed to be manually added or deleted.
Command Mode	Global configuration mode
Usage Guide	Add an HTTPS port. Use the **no** form of this command to delete an HTTPS port: **no content-audit https-port** *port-num.*

Configuration Example

Adding an HTTPS Port

Configuration	● Add HTTPS Port 4430.

Steps	
	FS# configure terminal FS(config)# content-audit https-port 4430 FS(url-obj-config)# end
Verification	● Run the **show content-audit https-port** command to display the configuration status.
	FS#show content-audit https-port HTTPS port information in user: 443 4430 HTTPS port information in kernel: 443 4430

Deleting an HTTPS Port

Configuration Steps	● Delete HTTPS Port 4430.
	FS# configure terminal FS(config)# no content-audit https-port 4430 FS(url-obj-config)# end
Verification	● Run the **show content-audit https-port** command to display the configuration status.
	FS#show content-audit https-port HTTPS port information in user: 443 HTTPS port information in kernel: 443

Common Errors

N/A

8.4.22 Enabling/Disabling HTTPS Audit

Configuration Effect

Enable HTTPS audit. The HTTPS audit function is used together with the content audit rule of each sub-service to audit and filter HTTPS encrypted websites.
Currently, only the HTTPS domain names can be audited and filtered, and the HTTPS audit function should be used together with URL rules.

Notes

Domain names in the access flows to the HTTPS encrypted websites can be audited and filtered only when the HTTPS audit function is used together with URL rules.

Configuration Steps

Enabling/Disabling HTTPS Audit

Mandatory. This function is configured to audit and filter the access to the HTTPS encrypted websites.

Verification

Run the show running-config command to display the configuration status.

Related Commands

Enabling/Disabling HTTPS Audit

Command	**https-audit enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Enable HTTPS audit. Use the **no** form of this command to disable HTTPS audit: **no https-audit enable**.

Configuration Example

Enabling HTTPS Audit

Configuration Steps	● Enable HTTPS audit.
	FS# configure terminal FS(config)# https-audit enable FS(url-obj-config)# end ● To audit and filter HTTPS domain names, configure URL rules. For example, enable the URL default audit rule. FS# configure terminal

	FS(config)# content-policy _AUDIT_DEFAULT FS(cont-plcy-config)# url-rule audit-default-enable FS(cont-plcy-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Disabling HTTPS Audit

Configuration Steps	● Disable HTTPS audit.
	FS# configure terminal FS(config)# no https-audit enable FS(url-obj-config)# end
Verification	● Run the **show running-config** command to display the configuration status.

Common Errors

N/A

8.4.23 Configuring Telnet Audit Rules

Configuration Effect

Enable the Telnet default audit function.
Add a Telnet audit rule to a content audit policy group.
Swap priorities of Telnet audit rules.

Notes

The validity status of a Telnet audit rule is subject to whether a time object is valid and whether a policy group to which the Telnet audit rule belongs is associated with a valid user.
In one policy group, a rule configured later has a higher priority.

Configuration Steps

Configuring Telnet Audit Rules

Mandatory.

Configuring Telnet Default Audit

Optional. This function is configured to enable the Telnet default audit.

Swapping Priorities of Telnet Audit Rules

Optional. This function is configured to swap priorities of Telnet audit rules.

Verification

Run the **show running-config** command to display the configuration status.

Related Commands

Configuring Telnet Audit Rules

Command	**telnet-rule** *rule-id* **time-range** *time-name* **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]
Parameter Description	*rule-id*: Specifies the ID of a rule. A value range is **1** to **200**, and a maximum of 200 rules are supported. *time-name*: Specifies the name of a time object in a rule validity period. *comment-string*: Specifies the description of a rule.
Command Mode	Content audit policy group configuration mode
Usage Guide	1. The ID of a rule must be unique in one content audit policy group, and can be repeated in another content audit policy group. 2. All access control rules in a content audit policy group are prioritized, and the last configured rule has the highest priority. 3. A rule is invalid when the time name associated with the rule does not exist. 4. Use the **no** form of this command to delete a Telnet access control rule: **no telnet-rule** *rule-id*.

Configuring Telnet Default Audit

Command	**telnet-rule audit-default-enable**
Parameter Description	N/A
Command Mode	Content audit policy group configuration mode
Usage Guide	1. The default audit function is valid only to a default audit group named **_AUDIT_DEFAULT**. This command is invalid to other policy groups. 2. Use the **no** form of this command to disable the Telnet default audit function: **no telnet-rule audit-default-enable**.

Deleting All Telnet Audit Rules in a Policy Group

Command	**telnet-rule delete-all**
Parameter Description	N/A
Command Mode	Content audit policy group configuration mode
Usage Guide	Use this command to delete all Telnet audit rules of the current policy group, without affecting other policy groups.

Swapping Priorities of Telnet Audit Rules

Command	**telnet-rule priority-swap** *rule-id1 rule-id2*
Parameter Description	*rule-id1*: Specifies the ID of rule 1 of which the priority is to be swapped. *rule-id2*: Specifies the ID of rule 2 of which the priority is to be swapped.
Command Mode	Content audit policy group configuration mode
Usage Guide	This priority swap command is used to swap priorities of two access control rules. After this command is run, run the **show running** command to display a change in ranks of the two rules. Output of the **show running** command does not display the priority swap command.

Configuration Example

Configuring Telnet Audit Rules

Configuration Steps	Add a Telnet audit rule to the content audit policy group policyA, to filter the posted files and audit the behavior.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# telent-rule 2 time-range any action deny audit comment TEST FS(cont-plcy-config)# end
	Delete all Telnet audit rules in the policy group policyA.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# telnet-rule delete-all FS(cont-plcy-config)# end
Verification	Run the **show running-config** command to display the configuration status.

Configuring Telnet Default Audit

Configuration Steps	Enable the Telnet default audit function.
	FS# configure terminal FS(config)# content-policy _AUDIT_DEFAULT FS(cont-plcy-config)# telnet-rule audit-default-enable FS(cont-plcy-config)# end
Verification	Run the **show running-config** command to display the configuration status.

Swapping Priorities of Telnet Audit Rules

Configuration Steps	Swap priorities of Telnet access control rules 10 and 20 in the policy group policyA.
	FS# configure terminal

	FS(config)# content-policy policyA FS(cont-plcy-config)# telnet-rule priority-swap 10 20 FS(cont-plcy-config)# end
Verification	Run the **show running-config** command to display the configuration status.

Common Errors

A repeated rule ID causes a configuration failure.

A rule is invalid because an object referenced by the rule does not exist.

An actual audit result is different from expectation because rule priorities are not cleared.

8.4.24 Configuring FTP Audit Rules

Configuration Effect

Enable the FTP default audit function.

Add an FTP audit rule to a content audit policy group.

Swap priorities of FTP audit rules.

Notes

The validity status of an FTP audit rule is subject to whether a referenced content object exists, whether a time object is valid, and whether a policy group to which the FTP audit rule belongs is associated with a valid user.

In one policy group, a rule configured later has a higher priority.

Configuration Steps

Configuring FTP Audit Rules

Mandatory.

Configuring FTP Default Audit

Optional. This function is configured to enable the FTP default audit.

Swapping Priorities of FTP Audit Rules

Optional. This function is configured to swap priorities of FTP audit rules.

Verification

Run the show running-config command to display the configuration status.

Related Commands

Configuring FTP Audit Rules

Command	**ftp-rule** *rule-id* **time-range** *time-name* [**filename** *content-object-name*] **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]
Parameter	*rule-id*: Specifies the ID of a rule. A value range is **1** to **200**, and a maximum of 200 rules are supported.

Description	*time-name*: Specifies the name of a time object in a rule validity period. *content-object-name*: Specifies the name of a content object used in a rule. *comment-string*: Specifies the description of a rule.
Command Mode	Content audit policy group configuration mode
Usage Guide	1. The ID of a rule must be unique in one content audit policy group, and can be repeated in another content audit policy group. 2. All access control rules in a content audit policy group are prioritized, and the last configured rule has the highest priority. 3. A rule is invalid when the time name or content object name associated with the rule does not exist. 4. Use the **no** form of this command to delete an FTP access control rule: **no ftp-rule** *rule-id*.

Configuring FTP Default Audit

Command	**ftp-rule audit-default-enable**
Parameter Description	N/A
Command Mode	Content audit policy group configuration mode
Usage Guide	1. The default audit function is valid only to a default audit group named **_AUDIT_DEFAULT**. This command is invalid to other policy groups. 2. Use the **no** form of this command to disable the FTP default audit function: **no ftp-rule audit-default-enable**.

Deleting All FTP Audit Rules in a Policy Group

Command	**ftp-rule delete-all**
Parameter Description	N/A
Command Mode	Content audit policy group configuration mode
Usage Guide	Use this command to delete all FTP audit rules of the current policy group, without affecting other policy groups.

Swapping Priorities of FTP Audit Rules

Command	**ftp-rule priority-swap** *rule-id1 rule-id2*
Parameter Description	*rule-id1*: Specifies the ID of rule 1 of which the priority is to be swapped. *rule-id2*: Specifies the ID of rule 2 of which the priority is to be swapped.
Command Mode	Content audit policy group configuration mode
Usage Guide	This priority swap command is used to swap priorities of two access control rules. After this command is run, run the **show running** command to display a change in ranks of the two rules. Output of the **show running** command does not display the priority swap command.

Enabling Uploaded File Content Audit Based on FTP Audit Rules

Command	**[no]ftp-upload-file-audit enable**
Parameter Description	
Command Mode	Content audit policy group configuration mode
Usage Guide	The default audit function is valid only to a default audit group named **_AUDIT_DEFAULT**. This command is invalid to other policy groups.

Configuration Example

Configuring FTP Audit Rules

Configuration Steps	Add an FTP audit rule to the content audit policy group policyA, to filter the posted files and audit the user behavior.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# ftp-rule 2 time-range any action deny audit comment TEST FS(cont-plcy-config)# end
	Delete all FTP audit rules in the policy group policyA.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# ftp-rule delete-all FS(cont-plcy-config)# end
Verification	Run the **show running-config** command to display the configuration status.

Configuring FTP Default Audit

Configuration Steps	Enable the FTP default audit function.
	FS# configure terminal FS(config)# content-policy _AUDIT_DEFAULT FS(cont-plcy-config)# ftp-rule audit-default-enable FS(cont-plcy-config)# end
Verification	Run the **show running-config** command to display the configuration status.

Swapping Priorities of FTP Audit Rules

Configuration Steps	Swap priorities of FTP access control rules 10 and 20 in the policy group policyA.
	FS# configure terminal FS(config)# content-policy policyA

	FS(cont-plcy-config)# ftp-rule priority-swap 10 20 FS(cont-plcy-config)# end
Verification	Run the **show running-config** command to display the configuration status.

Enabling Uploaded File Content Audit Based on FTP Audit Rules

Configuration Steps	Enable uploaded file content audit based on FTP audit rules.
	FS# configure terminal FS(config)# content-policy _AUDIT_DEFAULT FS(cont-plcy-config)# ftp-upload-file-audit enable FS(cont-plcy-config)# end
Verification	Run the **show running-config** command to display the configuration status.

Common Errors

A repeated rule ID causes a configuration failure.

A rule is invalid because an object referenced by the rule does not exist.

An actual audit result is different from expectation because rule priorities are not cleared.

8.4.25 Configures File Filtering Rules

Configuration Effect

Add a file filtering rule to a content audit policy group.

Swap priorities of file filtering rules.

Notes

The validity status of a file filtering rule is subject to whether a referenced content object exists, whether a time object is valid, and whether a policy group to which the file filtering rule belongs is associated with a valid user.

In one policy group, a rule configured later has a higher priority.

Configuration Steps

Configuring File Filtering Rules

Mandatory.

Swapping Priorities of File Filtering Rules

Optional. This function is configured to swap priorities of file filtering rules.

Verification

Run the **show running-config** command to display the configuration status.

Related Commands

Configuring File Filtering Rules

Command	**file-rule** *rule-id* **time-range** *time-name* **acti[1]on** { **permit** | **deny** } [**audit**] [**comment** *comment-string*] **file-rule** *rule-id* **relation** { **and** | **or** } [**file-name** *content-obj-string1*] [**file-type** *content-obj-string2*]
Parameter Description	*rule-id*: Specifies the ID of a rule. A value range is **1** to **200**, and a maximum of 200 rules are supported. *time-name*: Specifies the name of a time object in a rule validity period. *comment-string*: Specifies the description of a rule. *content-obj-string1*: Specifies the file name keyword. *content-obj-string2*: Specifies the file type keyword.
Command Mode	Content audit policy group configuration mode
Usage Guide	1. The ID of a rule must be unique in one content audit policy group, and can be repeated in another content audit policy group. 2. All access control rules in a content audit policy group are prioritized, and the last configured rule has the highest priority. 3. A rule is invalid when the time name, content object string 1, or content object string 2 associated with the rule does not exist. 4. Use the **no** form of this command to delete a file access control rule: **no file-rule** *rule-id*.

Swapping Priorities of File Filtering Rules

Command	**file-rule priority-swap** *rule-id1 rule-id2*
Parameter Description	*rule-id1*: Specifies the ID of rule 1 of which the priority is to be swapped. *rule-id2*: Specifies the ID of rule 2 of which the priority is to be swapped.
Command Mode	Content audit policy group configuration mode
Usage Guide	This priority swap command is used to swap priorities of two access control rules. After this command is run, run the **show running** command to display a change in ranks of the two rules. Output of the **show running** command does not display the priority swap command.

Configuration Example

Configuring File Filtering Rules

Configuration Steps	Add a file filtering rule to the content audit policy group policyA, to filter the posted files and audit the user behavior.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# file-rule 2 time-range any action deny audit comment TEST FS(cont-plcy-config)# file-rule 2 relation or file-name *file name keyword* FS(cont-plcy-config)# end

Swapping Priorities of File Filtering Rules

Configuration Steps	Swap priorities of file access control rules 10 and 20 in the policy group policyA.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# file-rule priority-swap 10 20 FS(cont-plcy-config)# end
Verification	Run the **show running-config** command to display the configuration status.

Deleting File Filtering Rules

Configuration Steps	Delete all file filtering rules in the policy group policyA.
	FS# configure terminal FS(config)# content-policy policyA FS(cont-plcy-config)# file-rule delete-all FS(cont-plcy-config)# end
Verification	Run the **show running-config** command to display the configuration status.

Common Errors

A repeated rule ID causes a configuration failure.

A rule is invalid because an object referenced by the rule does not exist.

An actual audit result is different from expectation because rule priorities are not cleared.

8.4.26 Enabling Attachment Upload to ELOG Server

Configuration Effect

By default, attachments cannot be uploaded to the ELOG server in NPE mode. Attachments can be uploaded to the ELOG server only after this function is enabled.

Notes

This function takes effect only in NPE mode.

Configuration Steps

Enabling Attachment Upload to ELOG Server

Optional. This function is enabled to upload attachments to the ELOG server in NPE mode.

Verification

Run the show running-config command to display the configuration status.

Related Commands

Enabling Attachment Upload to ELOG Server

Command	**content-audit attach-to-elog enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to enable attachment upload to the ELOG server. Use the **no** form of this command to disable attachment upload to the ELOG server: **no content-audit attach-to-elog enable**.

Configuration Example

Enabling Attachment Upload to ELOG Server

Configuration Steps	Enable attachment upload to the ELOG server in NPE mode.
	FS# configure terminal FS(config)# content-audit attach-to-elog enable FS(url-obj-config)# end
Verification	Run the **show running-config** command to display the configuration status.

Disabling Attachment Upload to ELOG Server

Configuration Steps	Disable attachment upload to the ELOG server.
	FS# configure terminal FS(config)# no content-audit attach-to-elog enable FS(url-obj-config)# end
Verification	Run the **show running-config** command to display the configuration status.

Common Errors

N/A

8.4.27 Enabling Content Audit Alarming

Configuration Effect

By default, content audit alarming is disabled by default. The content audit details will be sent to the specified mail address periodically after this function is enabled.

Notes

N/A

Configuration Steps

Enabling Content Audit Alarming

,Mandatory

Verification

Run the **show content-audit alarm config** command to display the configuration.

Related Commands

Enabling Content Audit Alarming

Command	**content-audit alarm enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use the **no** form of this command to disable content audit.

Configuration Example

Enabling Content Audit Alarming for All Types

Configuration Steps	Enable content audit alarming for all types.
	FS# configure terminal FS(config)# content-audit alarm type all FS(config)# end
Verification	Run the **show content-audit alarm config** command to display the configuration status.

Disabling Content Audit Alarming for All Types

Configuration Steps	Dsiable content audit alarming for all types.
	FS# configure terminal FS(config)# no content-audit alarm type all FS(config)# end
Verification	Run the **show content-audit alarm config** command to display the configuration.

Configuring a Mail Subject and Mail Address

Configuration Steps	Configure a mail subject and mail address.
	FS# configure terminal FS(config)# content-audit alarm mail subject alarming mail

	FS(config)# content-audit alarm mail to xxx@126.com
Verification	Run the **show content-audit alarm config** command to display the configuration.

Configuring a Mailing Cycle

Configuration Steps	Configure a mailing cycle.
	FS# configure terminal FS(config)# content-audit alarm mail cycle 5 FS(config)# end
Verification	Run the **show content-audit alarm config** command to display the configuration.

Common Errors

N/A

8.4.28 Configuring Content Audit Reporting

Configuration Effect

Configure a report creation time.
Enable or disable reporting.
Configure a custom report rule.

Notes

N/A

Configuration Steps

Configuring a Report Creation Time

Optional

Enabling Reporting

Optional

Configuring a Custom Report Rule

Optional

Verification

Run the **show report-create-time** command to display the report creation time.

Run the **show report-function** command to display whether reporting is enabled.

Run the **show report-custom-config** command to display the custom report rule.

Related Commands

Configuration Example

Configuring a Report Creation Time

Command	**report-create-time** *hh:mm:ss*
Parameter Description	*hh:mm:ss:* Configures a report creation time.
Command Mode	Global configuration mode
Usage Guide	Use the **no** form of this command to remove the configuration.

Enabling Reporting

Command	**report-function enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use the **no** form of this command to disable reporting.

Configuring a Custom Content Audti Rule

Command	**report-custom-config** *rule-id* **set-param report_name** *reportname* **top** *top-nu* **cycle** { **day** | **week** | **month** } { **usr-ip** | **usr-name** } *usr_name* **alarm** { **on** | **off** } { **sys-mail** | **custom-mail** *mail_adds* } **report-custom-config** *rule-id* **set-app** [**postfile**] [**url-cls**] [**url-host**] [**web-bbs**] [**web-search**] [**vid**] [**mail**] [**web-mail**] [**im**]
Parameter Description	*rule-id*: Configures a custom report rule ID. *reportname*: Configures a report name. *top-nu*: Displays Top N records. **cycle**: Configures a reporting cycle. **usr_name**: Configures a username or IP address. **alarm**: Enables alarming. **mail_adds**: Configures a mail address.
Command Mode	Global configuration mode
Usage Guide	Use the **no** form of this command to remove the configugration.

Configuration Example

Configuring a Report Creation Time

Configuration	Configure a report creation time.

Steps	
	FS# configure terminal FS(config)# report-create-time 02:00:00 FS(config)# end
Verification	Run the **show report-create-time** command to display the configuration.

Enabling Reporting

Configuration Steps	Enabling Reporting.
	FS# configure terminal FS(config)# report-function enable FS(config)# end
Verification	Run the **show report-function** command to display the configuration.

Configuring a Custom Report Rule

Configuration Steps	Configure a custom report rule.
	FS# configure terminal FS(config)# report-custom-config 1 set-param report-name report_usrA top 10 cycle day usr-name usrA alarm on custom-mail 123@126.com FS(config)# report-custom-config 1 set-app postfile web-search
Verification	Run the **show report-custom-config** command to display the configuration.

Common Errors

N/A

8.5 Monitoring

Clearing

Description	Command
Clears real-time statistics of content audit.	**clear content-audit statistics**

Displaying

Description	Command

Displays information about a content audit policy group.	**show content-policy** [**policy** [*policy-name*] | **stat** [**policy** policy-*name*]]
Displays association information between a user and a policy.	**show content-policy-relate policy-view** [{ **policy** *policy-name* | { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } | **ip** *A.B.C.D* } }] **show content-policy-relate user-view** { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } | **ip** *A.B.C.D* } [**detail**]
Displays information about system URL classes.	**show url-class system** [**class** { **id** *class-id* | **name** *class-name* }] **show url-class system comment** [**class** { **id** *class-id* | **name** *class-name* }] **show url-class system custom** [**class** { **id** *class-id* | **name** *class-name* }] **show url-class system exact**
Displays information about a designated system URL class.	**show url-class url** *url-string*
Displays information about a user-defined URL class.	**show url-class user-cfg** [*class-name*]
Displays information about a URL rule.	**show url-rule content-policy** *policy-name* [**subscriber** *subs-name*] [**auth-subscriber** *auth-subs-name*]
Displays details about application control audit.	**show app-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* | **bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**app-group** *app-group-name*] [**rule-name** *rule-name*] [**ip** *addr*] [**permit | deny**] **order-by** { **time | subscriber | internal-ip | app** } { **asc | desc** } [**start-item** *integer1* **end-item** *integer2*]
Displays statistics about application control audit.	**show app-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* | **bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**app-group** *app-group-name*] [**rule-name** *rule-name*] [**permit | deny**]
Displays IM audit details.	**show im-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* **| bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**direction** { **in** | **out** | **double** }] [**type** { **qq** | **msn** }] [**message** *keyword*] [**account** *account-string*] [**rule-name** *rule-name*] [**ip** *addr*] [**permit | deny**] **order-by** { **time | subscriber | auth-subscriber | internal-ip | direction** } { **asc | desc** } [**start-item** *integer1* **end-item** *integer2*]

Displays IM audit statistics.	**show im-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm::ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* | **bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**direction** { **in** | **out** | **double** }] [**type** { **qq** | **msn** }] [**message** *keyword*] [**account** *account-string*] [**rule-name** *rule-name*] [**ip** *addr*] [**permit** | **deny**]
Displays information about mail audit attachments.	**show mail-audit attachment-info timestamp** *timestamp* **rand-id** *rand-id*
Displays mail audit details.	**show mail-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* | **bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**direction** { **in** | **out** | **double** }] [**from** *keyword1*] [**to** *keyword2*] [**subject** *keyword3*] [**rule-name** *rule-name*] [**permit** | **deny**] **order-by** { **time** | **subscriber** | **auth-subscriber** | **internal-ip** | **direction** | **send-mail-addr** | **mail-size** } { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]
Displays mail audit statistics.	**show mail-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* | **bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**direction** { **in** | **out** | **double** }] [**from** *keyword1*] [**to** *keyword2*] [**subject** *keyword3*] [**rule-name** *rule-name*] [**permit** | **deny**]
Displays URL audit details.	**show url-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* | **bridge** *bridge-num*] [**subscriber** *subs-name*] [**auth-subscriber** *auth-subs-name*] [**ip** *addr*] [**url-class** *class-name* | **url-object** *obj-name* | **url** *url-string* | **url-host** *host-string1*] [**host** *host-string2*] [**permit** | **deny**] [**order-by time** | **url-class** | **url** | **host** | **ip**] { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]
Displays URL audit statistics.	**show url-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* | **bridge** *bridge-num*] [**subscriber** *subs-name*] [**auth-subscriber** *auth-subs-name*] [**ip** *addr*] [**url-class** *class-name* | **url-object** *obj-name*] [**host** *host-string*] [**permit** | **deny**]
Displays URL audit ranks.	**show url-audit top** *n* [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* | **bridge** *bridge-num*] [**subscriber** *subs-name*] [**auth-subscriber** *auth-subs-name*] [**url-class** *class-name* | **url-object** *obj-name*] [**host** *host-string*] [**permit** | **deny**] [**order-by time** | **url-class** | **url** | **url-class** | **host-times**]

Displays Web BBS audit details.	**show web-bbs-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* | **bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**content** *keyword*] [**rule-name** *rule-name*] [**permit** | **deny**] **order-by** { **time** | **subscriber** | **auth-subscriber** | **internal-ip** | **url** } { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]
Displays Web BBS audit statistics.	**show web-bbs-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm::ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* | **bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**content** *keyword*] [**rule-name** *rule-name*] [**permit** | **deny**]
Displays information about Web mail audit attachments.	**show web-mail-audit attachment-info timestamp** *timestamp* **rand-id** *rand-id*
Displays Web mail audit details.	**show web-mail-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* | **bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**direction** { **in** | **out** | **double** }] [**from** *keyword1*] [**to** *keyword2*] [**subject** *keyword3*] [**rule-name** *rule-name*] [**permit** | **deny**] **order-by** { **time** | **subscriber** | **auth-subscriber** | **internal-ip** | **direction** | **send-mail-addr** } { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]
Displays Web mail audit statistics.	**show web-mail-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* | **bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**direction** { **in** | **out** | **double** }] [**from** *keyword1*] [**to** *keyword2*] [**subject** *keyword3*] [**rule-name** *rule-name*] [**permit** | **deny**]
Displays Web search audit details.	**show web-search-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* | **bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**keyword** *keyword*] [**rule-name** *rule-name*] [**permit** | **deny**] **order-by** { **time** | **subscriber** | **auth-subscriber** | **internal-ip** | **url** } { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]
Displays Web search audit statistics.	**show web-bbs-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm::ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* | **bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**keyword** *keyword*] [**rule-name** *rule-name*] [**permit** | **deny**]

Displays virtual identity audit statistics.	**show vid-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**type** { **weibo** | **weixin** }] [**uid** *uid-string*] [**nickname** *nick-string*] [**ip** *addr1*] [**mac** *addr2*] **order-by** { **time** | **subscriber** | **auth-subscriber** | **internal-ip** | **uid** | **mac** } { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]
Displays virtual identity audit statistics.	**show im-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**type** { **weibo** | **weixin** }] [**uid** *uid-string*] [**nickname** *nick-string*] [**ip** *addr1*] [**mac** *addr2*]
Displays QQ audit details.	**show plugin-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* | **bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**content** *keyword*] [**rule-name** *rule-name*] [**permit** | **deny**] **order-by** { **time** | **subscriber** | **auth-subscriber** | **internal-ip** | **url** } { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]
Displays QQ audit statistics.	**show plugin-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm::ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* | **bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**content** *keyword*] [**rule-name** *rule-name*] [**permit** | **deny**]
Displays postfile audit details.	**show postfile-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* | **bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**content** *keyword*] [**rule-name** *rule-name*] [**permit** | **deny**] **order-by** { **time** | **subscriber** | **auth-subscriber** | **internal-ip** | **url** } { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]
Displays postfile audit statistics.	**show postfile-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm::ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* | **bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**content** *keyword*] [**rule-name** *rule-name*] [**permit** | **deny**]
Displays postfile attachment.	**show postfile-audit relate-id** *relate-id* **timestamp** *timestamp*

Displays HTTP POST audit details.	**show post-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* | **bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**content** *keyword*] [**rule-name** *rule-name*] [**permit** | **deny**] **order-by** { **time** | **subscriber** | **auth-subscriber** | **internal-ip** | **url** } { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]
Displays HTTP POST audit statistics.	**show post-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm::ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**interface** *intf-name* | **bridge** *bridge-num*] [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**content** *keyword*] [**rule-name** *rule-name*] [**permit** | **deny**]
Displays real-time statistics of content audit.	**show content-audit statistics** { **brief** | **counts** }
Displays the status of writing of content audit information into the local memory.	**show content-audit write-db**
Displays HTTP port information.	**show content-audit http-port**
Displays HTTPS port information.	**show content-audit https-port**
Displays content audit statistics.	**show content-audit deny-stat**{ **brief** | **counts**|**ip** }
Displays Telnet audit details.	**show telnet-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr1*] [**service-ip** *addr2*] [**conn** | **disconn**] [**rule-name** *rule-name*] [**permit** | **deny**] **order-by** { **time** | **subscriber** | **auth-subscriber** | **internal-ip** | **service-ip**} { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]
Displays Telnet audit statistics.	**show telnet-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm::ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr1*] [**service-ip** *addr2*] [**conn** | **disconn**] [**rule-name** *rule-name*] [**permit** | **deny**]
Displays FTP audit details.	**show ftp-audit detail** [**export**] { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm:ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**file-name** *keyword*] [**rule-name** *rule-name*] [**permit** | **deny**] **order-by** { **time** | **subscriber** | **auth-subscriber** | **internal-ip** } { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]
Displays FTP audit statistics.	**show telnet-audit stat** { **recent** *hours* | **time-range from** *yyyy mm dd hh:mm::ss* **to** *yyyy mm dd hh:mm:ss* | **day-interval** *yyyy mm dd* **to** *yyyy mm dd* [**hour-interval** *hour1* **to** *hour2* [*hour3* **to** *hour4*]] } [**subscriber** *subs-name1*] [**auth-subscriber** *subs-name2*] [**ip** *addr*] [**file-name** *keyword*] [**rule-name** *rule-name*] [**permit** | **deny**]

Displays custom report configuration.	**show report-custom-config** { *rule-id*}
Displays custom report data.	**show report-custom-data** *rule-id*

Debugging

Debugging information output occupies system resources. Disable the debugging switch after debugging is finished.

Description	Command
Enables the audit processing and tracing debugging switch for application control audit.	**debug app-control audit**
Enables the configuration processing and tracing debugging switch for application control audit.	**debug app-control config**
Enables the status and resource information display debugging switch for application control audit.	**debug app-control info**
Enables the audit processing and tracing debugging switch for URL audit.	**debug url-audit audit**
Enables the configuration processing and tracing debugging switch for URL audit.	**debug url-audit config**
Enables the status and resource information display debugging switch for URL audit.	**debug url-audit info**
Enables the audit processing and tracing debugging switch for IM audit.	**debug im-audit audit**
Enables the configuration processing and tracing debugging switch for IM audit.	**debug im-audit config**
Enables the status and resource information display debugging switch for IM audit.	**debug im-audit info**
Enables the audit processing and tracing debugging switch for mail audit.	**debug mail-audit audit**
Enables the configuration processing and tracing debugging switch for mail audit.	**debug mail-audit config**
Enables the status and resource information display debugging switch for mail audit.	**debug mail-audit info**
Enables the audit processing and tracing debugging switch for Web BBS audit.	**debug web-bbs-audit audit**
Enables the configuration processing and tracing debugging switch for Web BBS audit.	**debug web-bbs-audit config**
Enables the status and resource information display debugging switch for Web BBS audit.	**debug web-bbs-audit info**
Enables the audit processing and tracing debugging switch for	**debug web-mail-audit audit**

Web mail audit.	
Enables the configuration processing and tracing debugging switch for Web mail audit.	**debug web-mail-audit config**
Enables the status and resource information display debugging switch for Web mail audit.	**debug web-mail-audit info**
Enables the audit processing and tracing debugging switch for Web search audit.	**debug web-search-audit audit**
Enables the configuration processing and tracing debugging switch for Web search audit.	**debug web-search-audit config**
Enables the status and resource information display debugging switch for Web search audit.	**debug web-search-audit info**
Enables the audit processing and tracing debugging switch for virtual identity audit.	**debug vid audit**
Enables the audit processing and tracing debugging switch for HTTPS domain name audit.	**debug https-url audit**
Enables the configuration processing and tracing debugging switch for HTTPS domain name audit.	**debug https-url config**
Enables the status and resource information display debugging switch for HTTPS domain name audit.	**debug https-url info**

9 Configuring LINE-QUALITY

9.1 Overview

LINE-QUALITY detects the line quality and disables abnormal lines.

Generally, it is used in Internet cafes with multiple lines.

When a line is disconnected or unstable, LINE-QUALITY proactively disables the line to route the traffic from other normal lines and improve the user experience.

Protocols and Standards

N/A

9.2 Applications

Application	Description
Configuring Line Detection	Set a line detection method and disable abnormal lines.

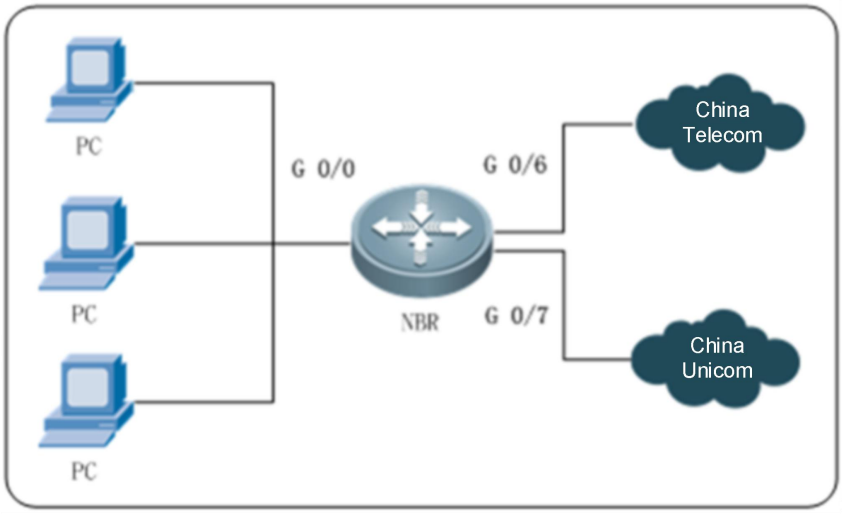
9.2.1 Line Detection

Scenario

The line detection function proactively detects whether lines are normal and disables abnormal lines to route application traffic from other normal lines and improve the user experience.

As shown in the following figure, the line of China Telecom is the primary line and the line of China Unicom is the secondary line. When the line of China Telecom is disconnected, applications routed through this line cannot be used. Because the line is the primary line, almost all applications are disconnected from the network. In this case, disable the G0/6 port to ensure that traffic is not routed through this line. After the line recovers, enable the G0/6 port.

Figure 9- 1



Remarks	NBR is an egress gateway. PCs are intranet clients that access the network through NBR. G0/0 is a LAN interface. G0/6 and G0/7 are WAN interfaces that are connected to the lines of China Telecom and China

	Unicom, respectively.

Deployment

Deploy line detection with track and RNS.

9.3 Features

Overview

Feature	Description
Line Detection Policy	Set a line detection method and disable abnormal lines.

9.3.1 Line Detection

The line detection function periodically detects whether lines are normal. When a line is abnormal, LINE-QUALITY proactively disables the line to route application traffic from a normal line and improve the user experience.

Working Principle

The line detection method is determined by RNS and track. When RNS detects that a line is abnormal, track notifies LINE-QUALITY. LINE-QUALITY disables the protocol of the line and instructs track and RNS to continue to detect lines. When the abnormal line recovers, LINE-QUALITY enables the protocol of the line.

9.4 Configuration

Configuration	Description and Command	
Configuring Line Detection Policy	Mandatory.	
	line-quality track enable	Enables LINE-QUALITY.
	line-quality track set log-only	Sets only to record the line detection result and not to enable or disable an interface.
	line-quality track set flow-gate *percent*	Sets not to disable an interface when the interface traffic reaches the threshold.
	line-quality track set interface *interface-name* **source** *ipaddr*	Sets the source IP address for monitoring line detection.
	line-quality track set timeout *msecs*	Sets the line detection timeout time.
	line-quality track set { up | down } frequency *f-secs* **delay** *d-secs*	Sets the line detection frequency and acknowledgment time.
	line-quality track permit-interface *interface-name*	Configures interfaces that can be detected.
	line-quality track interface *interface-name* **enable**	Enables detection for a line.
	line-quality track interface *interface-name* **icmp { enable | ip | url }**	Configures ICMP line detection.

	line-quality track interface *interface-name* **dns** **{ enable | ip }**	Configures DNS line detection.
	line-quality track interface *interface-name* **tcp** **{ enable | ip | url }**	Configures TCP line detection.

9.4.1 Configuring Line Detection Policy

Configuration Effect

Configure a line detection policy to disable a line when it is abnormal and enable the line when it recovers.

Notes

When there is only one line, line detection does not need to be configured.

Whether detection objectives are reachable needs to be verified in advance. Otherwise, misjudgment may occur.

You are advised to enable the "recording logs only" option first and check whether misjudgment occurs for a period of time. If not, disable this option.

Configuration Steps

Enabling Recording Logs Only

Optional.

Use the default value unless otherwise specified.

Command	**line-quality track set log-only**
Parameter Description	N/A
Defaults	The recording logs only function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Setting Not to Disable an Interface When the Interface Traffic Reaches the Threshold

Optional.

Use the default value unless otherwise specified.

Command	**line-quality track set flow-gate** *percent*
Parameter Description	*percent*: Indicates the percentage of traffic to the interface bandwidth.
Defaults	50%
Command Mode	Global configuration mode
Usage Guide	This configuration prevents detection packet loss due to full interface traffic, which will affect the line detection result.

Setting the Source IP Address for Line Detection

Optional.

Use the default value unless otherwise specified.

Command	**line-quality track set interface** *interface-name* **source** *ipaddr*
Parameter Description	*interface-name*: Indicates the interface name. *ipaddr*: Indicates the source IP address.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	This configuration ensures normal detection in special modes, for example, multiple WAN interfaces in the same network segment.

Setting the Line Detection Timeout Time

Optional.

Use the default value unless otherwise specified.

Command	**line-quality track set timeout** *msecs*
Parameter Description	*msesc*: Indicates the timeout time of each detection.
Defaults	2000 ms
Command Mode	Global configuration mode
Usage Guide	N/A

Setting the Line Detection Frequency and Acknowledgment Time

Optional.

Use the default value unless otherwise specified.

Command	**line-quality track set { up | down } frequency** *f-secs* **delay** *d-secs*
Parameter Description	*f-sesc*: Indicates the detection frequency. *d-secs*: Indicates the acknowledgment time when a new state is detected.
Defaults	Detection frequency
Command Mode	Global configuration mode
Usage Guide	The detection frequency and acknowledgment time vary depending on whether an interface is up or down. When an interface is up, the default detection frequency is 10s, timeout time is 2s, and acknowledgment time is 12s. Therefore, it takes a maximum of 24s (10s + 2s + 12s) to preliminarily determine whether the interface is normal. If the interface is detected as abnormal, the detection frequency is adjusted to 3s (frequency in down state). It takes a maximum of 17s (3s frequency + 2s timeout time + 12s acknowledgment time) to disable the interface. Then, the detection mode is changed to the interface down mode, and the whole process takes a maximum of 41s. When an interface is down, the default detection frequency is 3s, timeout time is 2s, and acknowledgment time is 60s. It takes a maximum of 65s (3s + 2s + 60s) to enable the interface.

	Generally, the acknowledgment time must be greater than or equal to the frequency plus the timeout time. In this case, at least another detection is performed during the acknowledgment period. This reduces frequent status change due to misjudgment.

Allowing Detection for a Line

Mandatory.

Command	**line-quality track permit-interface** *interface-name*
Parameter Description	*interface-name*: Indicates the name of an interface that allows detection.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	To configure a detection policy for an interface, you must first allow detection configuration. The interface must be a WAN interface. This command is to be used for display on a web page, and can be ignored.

Enabling Detection for a Line

Mandatory.

Command	**line-quality track interface** *interface-name* **enable**
Parameter Description	*interface-name*: Indicates the interface name.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	To configure a detection policy for an interface, enable detection for the interface first. If detection is disabled for an interface, existing configurations of the interface will be cleared.

Setting the Line Detection Protocol and Objective

Mandatory.

Command	**line-quality track interface** *interface-name* **icmp** { **enable** | *ip* | *url* } **line-quality track interface** *interface-name* **dns** { **enable** | *ip* } **line-quality track interface** *interface-name* **tcp** { **enable** | *ip* | *url* }
Parameter Description	*interface-name*: Indicates the interface name. **icmp**|**dns**|**tcp**: Indicates the protocol name. **enable**: Indicates that the protocol is enabled. *ip*: Indicates the IP address. *url*: Indicates the URL.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	When configuring the detection protocol and objective, first configure the IP address or URL of the detection objective and then enable the detection protocol. When the protocol detection is disabled, the configuration is

	not cleared. When the ICMP detection objective is not configured, the next-hop address is used as the objective by default. When ICMP is used to detect mainstream websites, you are advised to configure a DNS and TCP detection objective at the same time to prevent interface interruption due to misjudgment when the target server of ICMP detection forbids ping.

Manually Enabling or Disabling the Protocol for an Interface

Mandatory.

Command	**line-quality track interface** *interface-name* **up**
Parameter Description	*interface-name*: Indicates the interface name.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	When the detection result is incorrect, you can manually enable or disable an interface.

Verification

Display global configuration information.

Command	**show line-quality track**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	N/A
Command Presentation	FS#show line-quality track line quality track :disable line quality track log-only :off line quality track flow-gate :50% line quality track timeout :2000ms line quality track intf count:1[max:8] line quality track up :[freq:10 ; delay:12] line quality track down :[freq:30 ; delay:0] line quality permit interface: [3] GigabitEthernet 0/4 [4] GigabitEthernet 0/5 [5] GigabitEthernet 0/6

Display interface detection information.

Command	**show line-quality track interface** [*interface-name*]
Parameter Description	*interface-name*: Indicates the interface name.

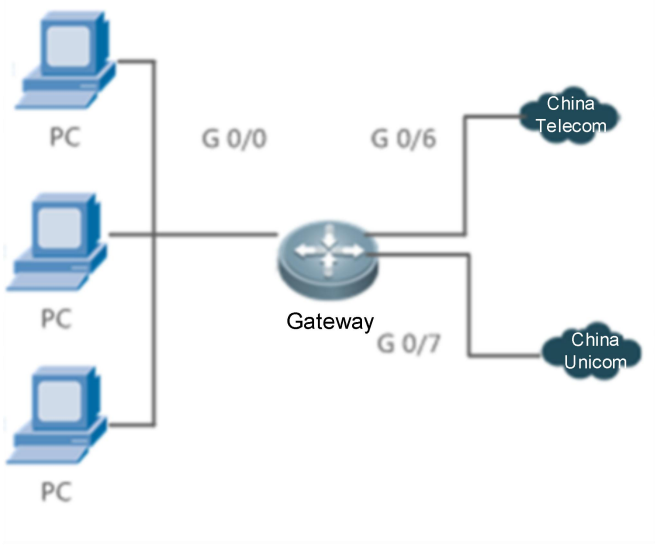
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	N/A
Command Presentation	FS#show line-quality track interface GigabitEthernet 0/5, index:4, stat:STOP, ctrl:NONE, source 0.0.0.0 ICMP: enable url: ip : 1.1.1.1 track_id : 0; rns_id: 0 track_msg: NONE; track_stat: NONE last time: DNS: enable ip : 1.1.1.1 track_id : 0; rns_id: 0 track_msg: NONE; track_stat: NONE last time: TCP: enable url: ip : 0.0.0.0 track_id : 0; rns_id: 0 track_msg: NONE; track_stat: NONE last time:

Display the interface control result.

Command	**show line-quality track interface line**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	
Command Presentation	FS#show line-quality track interface line Interface Status Protocol Last-ctrl GigabitEthernet 0/5 UP UP -- GigabitEthernet 0/6 UP UP --

Configuration Example

Configuring the G0/6 Interface to Use the ICMP and DNS Protocols for Detection

Scenario Figure 9- 2	
Configuration Steps	Enable LINE-QUALITY. Allow detection for the G0/6 interface. Enable detection for the G0/6 interface. Configure the ICMP and DNS detection objectives for the G0/6 interface. Enable ICMP and DNS detection for the G0/6 interface.
	FS#show line-quality track interface g 0/6 FS#config Enter configuration commands, one per line. End with CNTL/Z. FS(config)#line-quality track enable FS(config)#line-quality track permit-interface g 0/6 FS(config)#line-quality track interface g 0/6 enable FS(config)#line-quality track interface g 0/6 icmp www.baidu.com FS(config)#line-quality track interface g 0/6 dns 114.114.114.114 FS(config)#line-quality track interface g 0/6 icmp enable FS(config)#line-quality track interface g 0/6 dns enable FS(config)#exit FS#
Verification	Display detection information and status of an interface.
	FS#show line-quality track interface g 0/6

9.5 Monitoring

Displaying

Description	Command

Displays line quality information.	**show line-quality { detect | detail-detect } interface** *interface-name* **{{ recent** *hour* **} | { time-interval** *yyyy mm dd hh:mm* **to** *yyyy mm dd hh:mm* **}}**
Displays global configuration information for line detection.	**show line-quality track**
Displays line configuration information.	**show line-quality track interface** [*interface-name*]
Displays line control information.	**show line-quality track interface line**
Displays module running logs.	**show line-quality log** [**type** *type-num*] [**limit** *count*]

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Enables the line detection debugging switch.	**debug line-quality track**

Chapter 5 Device Management

1. Configuring Device Audit
2. Configuring USB
3. Configuring User Task
4. Configuring Service Manager

1 Configuring Device Audit

1.1 Overview

DEV-AUDIT (device audit) is used to monitor device running. This function periodically records information on usage of the CPU, memory, and hard disk of the device.

By viewing the records, users can learn system running information of the device in a certain period.

DEV-AUDIT information is recorded in the database of the SATA hard disk or internal storage. If no internal storage is available, logs can be sent to users.

1.2 Applications

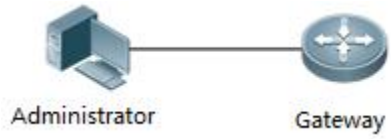
Application	Description
Enabling the Device Audit Function	The network administrator wants to learn device running information.

1.2.1 Enabling the Device Audit Function

Scenario

After the device audit function is enabled, devices periodically record CPU usage, memory, and hard disk space, allowing the administrator to learn device running information based on the record after the administrator logs in to the devices.

Figure 1-1



Remarks	The administrator logs in to the devices in Web mode to view device audit record.

Deployment

- Directly enable the function.

1.3 Features

Basic Concepts

CPU usage, memory usage, and hard disk usage

After the device audit function is enabled, devices read CPU usage, total memory, and available memory at an interval of five minutes, and calculate the memory usage. The devices also read the total space and available space of the flash and SATA hard disk at an interval of one hour. In the hard disk, data can be stored for 90 days.

Overview

Feature	Description
Enabling Device Audit	Enables the device audit function.

1.3.1 Enabling Device Audit

After the device audit function is enabled, devices periodically record running data for users to learn device running information.

Working Principle

After the device audit function is enabled, devices read CPU usage, total memory, and available memory at an interval of five minutes, and calculate the memory usage. The devices also read the total space and available space of the flash and SATA hard disk at an interval of one hour. In the hard disk, data can be stored for 90 days.

Related Configuration

Enabling the device audit function

This function is enabled by default.

1.4 Configuration

Configuration	Description and Command	
Enabling the Device Audit Function	Mandatory	
	dev-audit enable	Enables the device audit function.
Configuring Alarm Watermarks for Remaining Buffers of Device Audit	Optional	

1.4.1 Enabling the Device Audit Function

Configuration Effect

- Record information on usage of the CPU, memory, and hard disk of devices.

Notes

- Only devices with a SATA hard disk will record device audit data.

Configuration Steps

Enabling the device audit function

- Mandatory
- Enable this function on a local PC.

Verification

- Run a show command to display device audit record.

Related Commands

Enabling the device audit function

Command	dev-audit enable
Parameter	N/A

Description	
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Examples

Configuration Steps	● Enable the device audit function.
	FS# configure terminal FS(config)# dev-audit enable
Verification	Run a show command to display device audit record ten minutes later.
	FS# show dev-audit cpu from 2013 9 2 12:00:00 Date & Time CPU 2013-09-02 12:03:11 2% 2013-09-02 12:08:11 2%

1.4.2 Configuring Alarm Watermarks for Remaining Buffers of Device Audit

Configuration Effect

- Print an alarm log if the remaining buffers are insufficient.
- Print an alarm log if the number of **no buffer** alarms increases too fast within one minute.
- Print an alarm log if the usage of flow table connections is high.
- Print an alarm log if the usage of the flash or hard disk is high.

Notes

- N/A

Configuration Steps

↘ Enabling alarm watermarks of device audit

- Optional
- Enable this function on a local PC.

Verification

- Run a show command to display configuration result.

Related Commands

↘ Configuring alarm watermark for remaining buffers

Command	**dev-audit buffer high-watermark set up** *buffer-usage* **down** *buffer-usage*
Parameter Description	**up** *buffer-usage*: Specifies an upper watermark for the number of remaining buffers. When this value is reached, an alarm cancellation log is printed. The range is from 1 to 99, and the default value is 75. **down** *buffer-usage*: Specifies a lower watermark for the number of remaining buffers. When this value is reached, an alarm log is printed. The range is from 1 to 99, and the default value is 60.
Command Mode	Global configuration mode
Usage Guide	An alarm log is printed if the number of used buffers reaches the upper watermark. An alarm cancellation log is printed after the number of used buffers is smaller than the lower watermark. If available buffers are insufficient, Internet access of intranet users will be affected. The problem may be caused by device attacks.

Configuring alarm watermarks for the number of new no buffer alarms within one minute

Command	**dev-audit nobuffer high-watermark set up** *buffer-count* **down** *buffer-count*
Parameter Description	**up** *buffer-count*: Specifies an upper watermark for the number of new **no buffer** alarms for the device audit interface within one minute. When this value is reached, an alarm log is printed. The range is from 1 to 1,000,000, and the default value is 50,000. **down** *buffer-count*: Specifies a lower watermark for the number of new **no buffer** alarms for the device audit interface within one minute. When this value is reached, an alarm cancellation log is printed. The range is from 1 to 1,000,000, and the default value is 500.
Command Mode	Global configuration mode
Usage Guide	An alarm log is printed if the number of new **no buffer** alarms reaches the upper watermark within one minute. An alarm cancellation log is printed after the number of new **no buffer** alarms is less than the lower watermark. If new **no buffer** alarms increase too fast, Internet access of intranet users will be affected. The problem may be caused by device attacks.

Configuring alarm watermarks for the usage of flow table connections

Command	**dev-audit flow high-watermark set up** *unilization* **down** *unilization*
Parameter Description	**up** *unilization*: Specifies an upper watermark for the usage of flow table connections. When this value is reached, an alarm log is printed. The range is from 1 to 99 (in %), and the default value is 90. **down** *unilization*: Specifies a lower watermark for the usage of flow table connections. When this value is reached, an alarm cancellation log is printed. The range is from 1 to 99 (in %), and the default value is 75.
Command Mode	Global configuration mode
Usage Guide	An alarm log is printed if the usage of flow table connections reaches the upper watermark. An alarm cancellation log is printed after the usage of flow table connections is less than the lower watermark. If flow table connections are insufficient, Internet access of intranet users will be affected. The problem may be caused by device attacks.

Configuring alarm watermarks for the usage of the flash or hard disk

Command	**dev-audit flash high-watermark set up** *unilization* **down** *unilization*
Parameter Description	**up** *unilization*: Specifies an upper watermark for the usage of flash and hard disk. When this value is reached, an alarm log is printed. The range is from 1 to 99 (in %), and the default value is 90. **down** *unilization*: Specifies a lower watermark for the usage of flash and hard disk. When this value is reached, an alarm cancellation log is printed. The range is from 1 to 99 (in %), and the default value is 75.
Command Mode	Global configuration mode
Usage Guide	An alarm log is printed if the usage of the flash or hard disk reaches the upper watermark. An alarm cancellation log is printed after the usage of the flash or hard disk is less than the lower watermark. If the flash or hard disk is insufficient, some functions, for example, upgrade and audit record, may be unavailable.

Configuration Examples

Configuration Steps	● Set the alarm watermark to 90% and the alarm cancellation watermark to 75%.
	FS# configure terminal FS(config)# **dev-audit flash high-watermark set up** 90 **down** 75 Set flash high-watermark up 90% down 75%
Verification	Run the **show run** command to display the configuration.
	FS# show run **dev-audit flash high-watermark set up** 90 **down** 75

1.5 Monitoring

Displaying

Description	Command
Displays device audit record.	**show dev-audit** { **cpu** | **memory** | **flash** } **from** *year* [*month* [*mday* [*hh:mm:ss*]]] [**to** *year* [*month* [*mday* [*hh:mm:ss*]]]]

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs the device audit function.	**debug dev-audit errors**

2 Configuring USB

2.1 Overview

Universal serial bus (USB) is an external bus standard. In this document, USB refers to a USB-compliant peripheral device, for example, a USB flash drive.

USB is a hot swappable device. You can use it to copy files (such as configuration and log files) from a communication device, or copy external data (such as system upgrade files) to the flash of the communication device.

Specific application scenarios of the USB are detailed in configuration guides of related functions. This document describes only how to identify, use, and remove the USB and view information about the USB.

2.2 Applications

Application	Description
Using a USB Flash Drive to Upgrade a Device	Upgrade files are stored on a USB flash drive. After a device is powered on, the device detects the USB flash drive and runs the upgrade command to load the upgrade files. After loading is completed, the device is reset and runs the upgraded version.

2.2.1 Using a USB Flash Drive to Upgrade a Device

Scenario

Upgrade files are stored on a USB flash drive. After a device is powered on, the device detects the USB flash drive and runs the upgrade command to load the upgrade files. After loading is completed, the device is reset and runs the upgraded version. An example of the upgrade command is as follows:

upgrade usb0:/s12k-ppc_11.0(1B2)_20131025_main_install.bin

If the file is valid and execution of this command succeeds, the device will be automatically reset and run the upgraded version.

Deployment

- Use the prefix "usb0:/" to access USB 0. Run the **show usb** command to display information about the USB with the ID 0.
- Run the **upgrade** command to perform upgrade.

2.3 Features

➘ Using the USB

Insert a USB into the USB slot. The system automatically searches for the USB. After the USB is located, the driver module automatically initializes the driver of the USB. After initialization, the system automatically loads the file system on the USB. Later, the system can read or write this USB.

- If the system finds a USB and successfully loads the driver, the following information will be displayed:

```
*Jan    1 00:09:42: %USB-5-USB_DISK_FOUND: USB Disk <Mass Storage> has been inserted to USB port 0!
*Jan    1 00:09:42: %USB-5-USB_DISK_PARTITION_MOUNT: Mount usb0(type:FAT32),size : 1050673152B(1002MB)
```

"Mass Storage" indicates the name of the searched device, and "usb0:" indicates the first USB. "Size" indicates the size of the partition. For example, according to the preceding information displayed, the USB flash drive has a space of 1002 MB.

Removing the USB

Use a command line interface (CLI) command to remove the USB first; otherwise, an error may occur if the system is currently using the USB.

- If the USB is successfully removed, the following information will be displayed:

```
OK, now you can pull out the device 0.
```

You can remove the USB only after the preceding information is displayed.

2.4 Configuration

Configuration	Description and Command	
Using a USB	Mandatory.	
	N/A	
Removing a USB	(Mandatory) It is used to remove a USB.	
	usb remove	Removes a USB.

2.4.1 Using a USB

Configuration Effect

After a USB is loaded, you can run the file system commands (such as **dir**, **copy**, and **del**) to perform operations on the USB.

Notes

- The FS General Operating System (FSOS) is applicable only to devices (generally common USB flash drives) that support standard Small Computer System Interface (SCSI) commands. Other devices, such as the USB flash drive embedded in the USB network interface card (NIC) and USB flash drive with the virtual CD-ROM drive, cannot be used in the FSOS. Some devices are configured with the function of converting a USB port to the serial port.
- The USB supports only the FAT file system. Other file systems on the USB must be formatted to the FAT file system on a PC before the USB can be used on a device.
- The FSOS supports the hub. When a USB flash drive is inserted to a port on a hub, the access path becomes different. If the USB flash drive is inserted to a USB port on a device, the access path is **usbX:/**, where **X** indicates the device ID. You can run the **show usb** command to display this path. If the USB flash drive is inserted to a USB port through a hub, the access path is **usbX-Y:/**, where **X** indicates the device ID, and **Y** indicates the hub port ID. For example, **usb0-3:/** indicates port 3 on the hub that is connected to USB port 0 on the device.

Configuration Steps

Identifying a USB

A USB can be directly inserted to the USB slot without a CLI operation.

Using a USB

Perform the following operations to copy files from a USB to the flash:

- Run the **cd** command to enter the partition of the USB.
- Run the **copy** command to copy files on the USB to the flash on the device.
- Run the **dir** command to check whether the files are copied to the device.

If the USB has multiple partitions, you can access only the first FAT partition on the device.

The path of the USB does not contain any upper-level directory. After running the **cd usbX:** command to access a USB, you can run the **cd flash:** command to return to the flash file system.

Verification

Run the **show usb** command to display information about the USB inserted to the device.

Configuration Example

Using a USB Flash Drive

Scenario	Standalone environment
Configuration Steps	• Insert the USB flash drive into the USB slot of the device. • Run the **show usb** command on the device console. • Copy the **config.txt** file from the USB flash drive to the flash on the device.
	FS#show usb Device: Mass Storage ID: 0 URL prefix: usb0 Disk Partitions: usb0(type:vfat) Size:15789711360B(15789.7MB) Available size:15789686784B(15789.6MB) FS# FS# FS#dir usb0:/ Directory of usb0:/ 1 -rwx 4 Tue Jan 1 00:00:00 1980 fac_test 2 -rwx 1 Mon Sep 30 13:15:48 2013 config.txt 2 files, 0 directories 15,789,711,360 bytes total (15,789,686,784 bytes free)

	FS# FS# FS#copy usb0:/config.txt flash:/ Copying: ! Accessing usb0:/config.txt finished, 1 bytes prepared Flushing data to flash:/config.txt... Flush data done FS# FS#
Verification	● Check whether the **config.txt** file exists on the flash.

```
FS#
FS#dir flash:/
Directory of flash:/
    1 drw-          160   Wed Mar 31 08:40:01 2010   at
    2 drwx          160   Thu Jan   1 00:00:11 1970   dm
    3 drwx          160   Thu Jan   1 00:00:05 1970   rep
    4 drwx          160   Mon Apr 26 03:42:00 2010   scc
    5 drwx          160   Wed Mar 31 08:39:52 2010   ssh
    6 drwx          224   Thu Jan   1 00:00:06 1970   var
    7 d---          288   Sat May 29 06:07:45 2010   web
    8 drwx          160   Thu Jan   1 00:00:11 1970   addr
    9 drwx          160   Sat May 29 06:07:44 2010   cwmp
   10 drwx          784   Sat May 29 06:07:47 2010   sync
   11 --w-           92   Tue Feb   2 01:06:55 2010   config_vsu.dat
   12 -rw-          244   Sat Apr   3 04:56:52 2010   config.text
   13 -rwx            1   Thu Jan   1 00:00:30 1970   .issu_state
   14 -rw-            0   Tue Feb   2 01:07:03 2010   ss_ds_debug.txt
   15 -rw-         8448   Thu Jan   1 00:01:41 1970   .shadow
   16 -rwx          268   Thu Jan   1 00:01:41 1970   .pswdinfo
   17 -rw-            4   Tue May 25 09:12:01 2010   reload
   18 drwx          232   Wed Mar 31 08:40:00 2010   snpv4
   19 drwx         6104   Sat May 29 06:10:45 2010   .config
   20 ----            1   Thu Jan   1 00:04:51 1970   config.txt
   21 d---          160   Thu Jan   1 00:00:12 1970   syslog
   22 drwx          160   Tue May 25 03:05:01 2010   upgrade_ram
   23 drwx          160   Tue Feb   2 01:06:54 2010   dm_vdu
   24 -rwx           16   Thu Jan   1 00:01:41 1970   .username.data
9 files, 15 directories
5,095,424 bytes total (4,960,256 bytes free)
FS#
```

Common Errors

- Insert a USB flash drive that supports non-SCSI commands to the device.
- The USB does not use the FAT file system, and cannot be identified by the system.

2.4.2 Removing a USB

Configuration Effect

Remove the USB and ensure that the USB and the device are intact.

Notes

- Run the **usb remove** command before removing the USB; otherwise, a system error occurs.

Configuration Steps

Running the Remove Command

- Mandatory.
- Run the **usb remove** command before removing the USB.

Removing the USB

After the remove command is executed, remove the USB.

Verification

Run the **show usb** command to display information about the USB inserted to the device.

Related Commands

Removing a USB

Command	**usb remove** *device-id*
Parameter Description	*device-id*: Indicates the ID of the USB port on the device. You can run the **show usb** command to display this ID.
Command Mode	Privileged EXEC mode
Usage Guide	Before removing a USB, run the **usb remove** command; otherwise, an error occurs if the USB is in use. If the command is executed, related information will be displayed, and you can remove the USB. If the command execution fails, the USB is in use. In this case, do not remove the USB until it is not in use.

Configuration Example

Removing a USB

Scenario	Standalone environment
Configuration Steps	• Run the **show usb** command to display the ID of the USB. • Run the **usb remove** command to remove the USB.

	FS#show usb Device: Mass Storage ID: 0 URL prefix: usb0 Disk Partitions: usb0(type:vfat) Size:15789711360B(15789.7MB) Available size:15789686784B(15789.6MB) FS# FS# FS#usb remove 0 OK, now you can pull out the device 0.
Verification	● Run the **show usb** command again to check whether the USB is removed. If the device with ID 0 is not displayed in output of the **show usb** command, the USB is removed.
	FS#show usb FS#

2.5 Monitoring

Displaying

Description	Command
Displays information about the inserted USB.	**show usb**

3 Configuring User Task

3.1 Overview

USER-TASK (user task) is used to periodically run specified CLI commands. This function runs CLI commands at a specified time point after required CLI commands are configured, enabling unattended services.

3.2 Applications

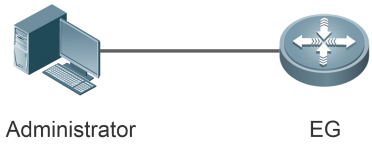
Application	Description
Restarting Devices Periodically	The network administrator wants that devices are restarted at specified time each week.
Collecting Device Information	The network administrator or technical engineers plans to run **show** commands periodically to collect required information.

3.2.1 Restarting Devices Periodically

Scenario

The network administrator expects that gateways are restarted at 2 a.m. each Sunday when network maintenance is performed.

Figure 3-1



Remarks	The administrator logs in to the devices in Web mode to configure the devices.

Deployment

- Enable the user task function.
- Set the restart time of the devices to 2 a.m. each Sunday.

3.2.2 Collecting Device Information

Scenario

The network administrator or technical engineer runs show commands periodically and log in to the devices to view the command execution result, expecting that device information is collected in a timely manner even if faults such as network interruption and TTY timeout occur when they run scripts over Telnet.

Figure 3-2

Remarks	The administrator logs in to the devices in Web mode to configure the devices.

Deployment

- Enable the user task function.
- Enable the user task log function.
- Configure show commands that to be executed.
- Log in to the devices to display the execution result.

3.3 Features

Basic Concepts

User task log

After the user task log function is enabled, execution results of all tasks (notwithstanding success or failure), as well as the task plan time and execution time will be recorded for users.

Command mode

Command modes fall into privileged EXEC mode and global configuration mode. If the privileged EXEC mode is used, commands starting with FS# are used to run show commands. If the global configuration mode is used, commands starting with **FS(config)#** are used to configure commands.

Command sequence

Some commands must be configured in different modes. For example, to add an application to or delete an application from a user-defined application group, run the following commands in sequence:

```
FS(config)#identify-application custom-group test_group
FS(config-custom-group)#app-add #app-add Instant messenger
```

These commands constitute a command sequence. On the CLI, commands that are used to add a task must be separated by the symbol @ in sequence.

Overview

Feature	Description
Configuring User Tasks	Enables the user task function, configures user tasks, and runs the CLI commands in the tasks.

3.3.1 Configuring User Tasks

After the user task function is enabled, the device runs CLI commands periodically according to the configured user tasks.

Working Principle

After user tasks are configured, the device will record task information in the task database. If the user task function is enabled, the device will read the task information from the task database each minute, invoke due tasks, and run the CLI commands one after another. If the user task log function is enabled as well, the device will record the execution result of the CLI command.

Related Configuration

Enabling the user task function

The user task function is enabled by default.

Use the **user-task enable** command to enable the user task function.

If the user task function is disabled, user tasks can still be added, modified or deleted, but the tasks in the task database will not be executed.

Enabling the user task log function

The user task log function is disabled by default.

Use the **user-task log enable** command to enable the user task log function.

If the user task log function is disabled, task execution result will not be recorded, but logs of previous tasks can be displayed.

3.4 Configuration

Configuration	Description and Command	
Configuring User Tasks	(Mandatory) It is used to add, delete, or modify tasks.	
	user-task enable	Enables the user task function.
	user-task	Configures user tasks.
Configuring User Task Logs	(Optional) It is used to configure the user task log function.	
	user-task log	Enables the user task log function.

3.4.1 Configuring User Tasks

Configuration Effect

- Run required CLI commands at a specified time according to the user tasks added.

Notes

- Configured user tasks can be invoked after the user task function is enabled.
- Up to 1000 tasks can exist at the same time.

Configuration Steps

Enabling the user task function

- Mandatory

Configuring user tasks

- Mandatory
- Add, delete, or modify user tasks on devices.

Verification

- Run a show command to display information in the user task database.

Related Commands

Enabling the user task function

Command	**user-task enable**
Parameter Description	N/A
Command mode	Global configuration mode
Usage Guide	N/A

Adding user tasks

Command	**user-task add** *task-name* **command** *cli-string* **mode** { **exec** | **config** } [**date** *YYYY MM DD*] **time** *hh:mm* [**every** { *mmm* / *hhh:mm* }]
Parameter Description	*task-name*: Configures a task name. ***command*** *cli-string*: Configures CLI commands or command sequence to be run. **exec**: Specifies the privileged EXEC mode. **config**: Specifies the global configuration mode. **date** *YYYY MM DD*: Configures a task execution date. **time** *hh:mm*: Configures the task execution time. **every** { *mmm* / *hhh:mm* }: Configures the task cycle time.
Command mode	Privileged EXEC mode
Usage Guide	This command is used to add user tasks. A CLI command that contains space must be enclosed by double quotation marks, and commands of a sequence must be separated using the symbol @. If a command contains the symbol @, use \@ instead to distinguish it from the separator. If no task date is specified, task execution date is set to current day by default. If task time is earlier than current time, task execution time is set to next day. If no cycle time is configured, the task will not be repeated. The parametric values can be modified using modify commands. If the configured task date and time is earlier than the current date and time, the configured task will be executed immediately, including the reload command.

Deleting user tasks

Command	**user-task delete** *task-name*
Parameter Description	*task-name:* Configures a task name.
Command mode	Privileged EXEC mode
Usage Guide	N/A

Modifying user tasks

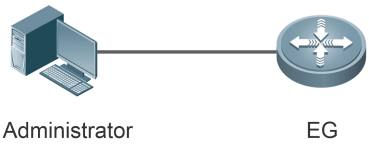
Command	**user-task modify** *task-name* { **mode** { **exec** | **config** } | **date** *YYYY MM DD* | **time** *hh:mm* | **every** { *mmm* / *hhh:mm* } }
Parameter Description	*task-name:* Configures a task name. **exec**: Specifies the privileged EXEC mode. **config**: Specifies the global configuration mode. **date** *YYYY MM DD*: Configures a task execution date. **time** *hh:mm*: Configures the task execution time. **every** { *mmm* / *hhh:mm* }: Configures the task cycle time.
Command mode	Privileged EXEC mode
Usage Guide	This command is used to modify attributes of specified tasks. If multiple attributes (for example, task time and cycle time) of a task need to be modified, you should modify the attributes one after another.

Displaying information in the user task database

Command	**show user-task**
Parameter Description	N/A
Command mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	This command is used to check whether a task is successfully added, deleted, or modified. This command is used to check whether the user task function and user task log function are enabled.

Configuration Examples

Configuring device restart time

Scenario **Figure 3-3**	
Configuration Steps	● Enable the user task function, and add a task to set the device restart time to 2 a.m. each Sunday. This reload command must be confirmed by entering yes, so the configuration needs a command sequence to complete.

	FS# configure terminal FS(config)# user-task enable FS(config)# exit FS# user-task add restart task command “reload@y” mode exec date 2014 9 21 time 2:00 every 168
Verification	● Run a show command to display information in the user task database. ● Run the **show version** command to check whether the devices are restarted at the specified restart time.
	FS# show user-task User-task: enable User-task log: unable Time Name Mode Loop Command-sequence 2014-09-21 02:00 restart task exec 168h reload y

Common Errors

- A CLI command is not enclosed by quotation marks.
- CLI commands of a sequence are not separated using the symbol @.
- Task name is too long.
- Task names are repeated.
- A task to be deleted or modified does not exist.
- Modification fails if the entered date and time is earlier than the current date and time.
- Database error occurs if a device does not have a hard disk.

3.4.2 Configuring User Task Logs

Configuration Effect

- Record task execution result.

Notes

- The user task function must be configured.
- Logs can be stored for 30 days at most.
- Maximum log size is 20 MB. If new logs are generated, old logs will be automatically cleared in sequence.

Configuration Steps

- Enable the user task log function.

Verification

- Run a show command to display user task log information.

Related Commands

Enabling the user task log function

Command	**user-task log enable**
Parameter Description	N/A
Command mode	Global configuration mode
Usage Guide	N/A

Displaying user task log information

Command	**show user-task log**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	N/A

Configuration Examples

Enabling the user task log function and displaying user task log information

Configuration Steps	• Configure user tasks (This step has been described before so it is not described again). • Enable the user task log function and display user task log information.
	FS# configure terminal FS(config)# user-task log enable FS(config)# exit FS# show user-task log

	---------- Task name: vvvv Task time: 2014-09-19 16:09 Execute time: 2014-09-19 15:09 Execute mode: exec Command: #wri Result: # Building configuration... [OK] ---------- Task name: Define an application group. Task time: 2014-09-18 19:03 Execute time: 2014-09-19 15:14 Execute mode: config Command: #identify-application custom-group test-group Command: #app-add Browse general web pages. Command: #app-add Instant messenger
Verification	N/A

3.5 Monitoring

Clearing

Description	Command
Clears user task logs.	**clear user-task**

Displaying

Description	Command
Displays information in the user task database.	**show user-task**
Displays user task log information.	**show user-task log**

4 Configuring SERVICE-MANAGER

4.1 Overview

Service Manager allows you to enable required service functions provided by a device.

Service functions provided by a device are used based on the application scenario, and some functions may not be used. These unused functions are loaded during device startup by default and will consume device resources. Unused web pages will affect other common functions as well, resulting in poor ease of use. Service Manager allows you to load service function components based on your actual requirements. In this case, you can prevent unconfigured service functions from running to save memory, reduce CPU consumption, and not present unwanted web pages.

Protocols and Standards

- N/A

4.2 Applications

Application	Description
Enabling or Disabling Services	Load service functions based on actual requirements.

4.2.1 Enabling or Disabling Services

Scenario

Configure the gateway based on functions required in actual scenarios. Disable functions that do not need to be used in Service Manager to release device resources and simplify menus on web UIs.

Figure 4- 1

Deployment

- Determine the services to be enabled or disabled.
- Configure the service status.

4.3 Features

Basic Concepts

Enabling or Disabling Services

To enable or disable a service, load or unload the processes of the service module, control whether the service module is loaded upon device startup, and display or screen specific web pages.

Overview

Feature	Description
Enabling or Disabling Services	Enable or disable a specific service.

4.3.1 Enabling or Disabling Services

Load services based on actual requirements to release device resources and simplify menus on web UIs.

- Loading or unloading some services takes effect after the device is restarted.
- After a service function is disabled, the service module is unloaded and related CLIs become unavailable.
- Note whether enabling multiple services will cause high memory usage of a device.

Working Principle

To enable or disable a service, load or unload the processes of the service module, control whether the service module is loaded upon device startup, and display or screen specific web pages.

Related Configuration

Enabling a Specific Service

Specify the service name to enable the service.

Disabling a Specific Service

Specify the service name to disable the service.

4.4 Configuration

Configuration	Description and Command	
Enabling or Disabling Services	Optional.	
	servctl service *name* { **on** | **off** }	Enables or disables a service.
	no servctl service *name*	Restores the default service status.

4.4.1 Enabling or Disabling Services

Configuration Effect

- Specify the service name to enable the service.
- Specify the service name to disable the service.
- Restore the default service status.

Notes

- Loading or unloading some services takes effect after the device is restarted.
- After a service function is disabled, the service module is unloaded and related CLIs become unavailable.
- Note whether enabling multiple services will cause high memory usage of a device.

Configuration Steps

Enabling or Disabling Services

- Optional. If enabling or disabling services is not configured, whether a service runs upon device startup is subject to the default settings of the current device version.
- If a function is not required, disable the corresponding service.

Command	**servctl service** *name* { **on** | **off** }
Parameter Description	*name*: Indicates the service name. To display the service name, run the show command. **on**: Sets the service status to Running. **off**: Sets the service status to Stop.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

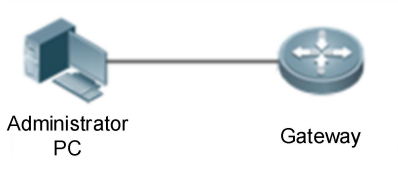
- Run the show command to display the service status.

Command	**show servctl** { **all** | **service** *name* }
Parameter Description	**all**: Displays the status of all services. **service** *name*: Displays the status of a specific service.
Command Mode	Privileged EXEC mode or global configuration mode
Usage Guide	This command is used to display services that can be controlled by Service Manager and the service status.
Command Presentation	FS#show servctl service was service controllable startup running ---------- ---------- --------- --------- was true true true

For details about the show command, see the command manual of the corresponding feature.

Configuration Example

Enabling the was Service to Run Upon Device Startup

Scenario **Figure 4- 2**	
Configuration Steps	Enable the was service. Loading or unloading the was service requires the device to restart. Restart the device for the service to take effect.
	FS(config)#servctl service was on You must reload the system to enable service was. FS(config)#exit FS#write FS#reload Reload system?(Y/N)
Verification	Run the show command to display the service status.
	FS#show servctl service was service controllable startup running ---------- ---------- --------- --------- was true true true

Common Errors

- The specified service name is incorrect, or the service cannot be controlled.

4.5 Monitoring

Displaying

Description	Command
Displays services that can be controlled by Service Manager and the service status.	**show servctl** { **all** | **service** *name* }

Chapter 6 IP Address & Application Configuration

1. Configuring IP Addresses and Services
2. Configuring ARP
3. Configuring IP Event Dampening
4. Configuring TCP
5. Configuring IPv4/IPv6 REF
6. Configuring Tunnel
7. Configuring FPM
8. Configuring NAT
9. Configuring MLLB
10. Configuring User Route

1 Configuring IP Addresses and Services

1.1 Overview

Internet Protocol (IP) sends packets to the destination from the source by using logical (or virtual) addresses, namely IP addresses. At the network layer, routers forward packets based on IP addresses.

Protocols and Standards

- RFC 1918: Address Allocation for Private Internets
- RFC 1166: Internet Numbers

1.2 Applications

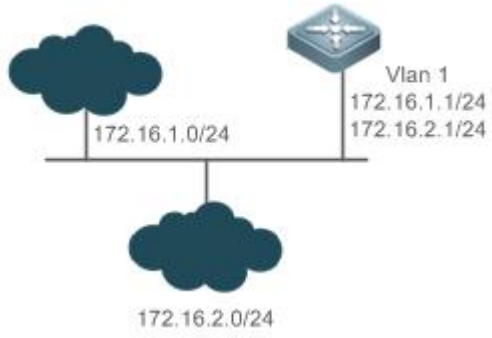
Application	Description
Configuring an IP Address for Communication	Two networks communicate through one switch interface.

1.2.1 Configuring an IP Address for Communication

Scenario

A switch is connected to a Local Area Network (LAN), which is divided into two network segments, namely, 172.16.1.0/24 and 172.16.2.0/24. Computers in the two network segments can communicate with the Internet through switches and computers between the two network segments can communicate with each other.

Figure 1- 1Configuring IP Addresses



Deployment

- Configure two IP addresses on VLAN1. One is a primary IP address and the other is a secondary IP address.
- On hosts in the network segment 172.16.1.0/24, set the gateway to 172.16.1.1; on hosts in the network segment 172.16.2.0/24, set the gateway to 172.16.2.1.

1.3 Features

Basic Concepts

IP Address

An IP address consists of 32 bits in binary. To facilitate writing and description, an IP address is generally expressed in decimal. When expressed in decimal, an IP address is divided into four groups, with eight bits in each group. The value range of each group is from 0 to 255, and groups are separated by a full stop ".". For example, "192.168.1.1" is an IP address expressed in decimal.

IP addresses are used for interconnection at the IP layer. A 32-bit IP address consists of two parts, namely, the network bits and the host bits. Based on the values of the first several bits in the network part, IP addresses in use can be classified into four classes.

For a class A address, the most significant bit is 0.7 bits indicate a network ID, and 24 bits indicate a local address. There are 128 class A networks in total.

Figure 1- 2

		8	16 24 32
Class A IP address	0	Network ID	Host ID

For a class B address, the first two most significant bits are 10.14 bits indicate a network ID, and 16 bits indicate a local address. There are 16,348 class B networks in total.

Figure 1- 3

			8	16 24 32
Class B IP address	1	0	Network ID	Host ID

For a class C address, the first three most significant bits are 110.21 bits indicate a network ID, and 8 bits indicate a local address. There are 2,097,152 class C networks in total.

Figure 1- 4

				8	16 24 32
Class C IP address	1	1	0	Network ID	Host ID

For a class D address, the first four most significant bits are 1110 and other bits indicate a multicast address.

Figure 1- 5

					8	16 24 32
Class D IP address	1	1	1	0	Multicast address	

The addresses with the first four most significant bits 1111 cannot be assigned. These addresses are called class E addresses and are reserved.

When IP addresses are planned during network construction, IP addresses must be assigned based on the property of the network to be built. If the network needs to be connected to the Internet, users should apply for IP addresses to the corresponding agency. In China, you can apply to China Internet Network Information Center (CNNIC) for IP addresses. Internet Corporation for Assigned Names and

Numbers (ICANN) is the final organization responsible for IP address assignment. If the network to be built is an internal private network, users do not need to apply for IP addresses. However, IP addresses cannot be assigned at random. It is recommended to assign dedicated private network addresses.

The following table lists reserved and available addresses.

Class	Address Range	Status
Class A network	0.0.0.0 - 0.255.255.255	Reserved
	1.0.0.0 - 126.255.255.255	Available
	127.0.0.0 - 127.255.255.255	Reserved
Class B network	128.0.0.0 - 191.254.255.255	Available
	191.255.0.0 - 191.255.255.255	Reserved
Class C network	192.0.0.0 - 192.0.0.255	Reserved
	192.0.1.0 - 223.255.254.255	Available
	223.255.255.0 - 223.255.255.255	Reserved
Class D network	224.0.0.0 - 239.255.255.255	Multicast address
Class E network	240.0.0.0 - 255.255.255.254	Reserved
	255.255.255.255	Broadcast address

Three address ranges are dedicated to private networks. These addresses are not used in the Internet. If the networks to which these addresses are assigned need to be connected to the Internet, these IP addresses need to be converted into valid Internet addresses. The following table lists private address ranges. Private network addresses are defined in RFC 1918.

Class	Address Range	Status
Class A network	10.0.0.0 - 10.255.255.255	1 class A network
Class B network	172.16.0.0 - 172.31.255.255	16 class B networks
Class C network	192.168.0.0 - 192.168.255.255	256 class C networks

For assignment of IP addresses, TCP/UDP ports, and other codes, refer to RFC 1166.

Subnet Mask

A subnet mask is also a 32-bit value. The bits that identify the IP address are the network address. In a subnet mask, the IP address bits corresponding to the bits whose values are 1s are the network address, and the IP address bits corresponding to the bits whose values are 0s are the host address. For example, for class A networks, the subnet mask is 255.0.0.0. By using network masks, you can divide a network into several subnets. Subnetting means to use some bits of the host address as the network address, thus decreasing the host capacity, and increasing the number of networks. In this case, network masks are called subnet masks.

Broadcast Packet

Broadcast packets refer to the packets destined for all hosts on a physical network. FS products support two types of broadcast packets: (1) directed broadcast, which indicates that all hosts on the specified network are packet receivers and the host bits of a destination address are all 1s; (2) limited broadcast, which indicates that all hosts on all networks are packet receivers and the 32 bits of a destination address are all 1s.

ICMP Packet

Internet Control Message Protocol (ICMP) is a sub-protocol in the TCP/IP suite for transmitting control messages between IP hosts and network devices. It is mainly used to notify corresponding devices when the network performance becomes abnormal.

TTL

Time To Live (TTL) refers to the number of network segments where packets are allowed to pass before the packets are discarded. The TTL is a value in an IP packet. It informs the network whether packets should be discarded as the packets stay on the network for a long time.

Features

Feature	Description
IP Address	The IP protocol can run on an interface only after the interface is configured with an IP address.
Broadcast Packet Processing	Broadcast addresses are configured and broadcast packets are forwarded and processed.
Sending ICMP Packets	ICMP packets are sent and received.
Limiting Transmission Rate of ICMP Error Packets	This function prevents Denial of Service (DoS) attacks.
IP MTU	Maximum Transmission Unit (MTU) of IP packets on an interface is configured.
IP TTL	The TTL of unicast packets and broadcast packets is configured.
IP Source Route	Source routes are checked.
IP Address Pool	An IP address is assigned to the peer end during PPP negotiation.

1.3.1 IP Address

IP addresses are obtained on an interface in the following ways:

3. Manually configuring IP addresses
4. Obtaining IP addresses through DHCP
5. Obtaining IP addresses through PPP negotiation
6. Borrowing IP addresses of other interfaces

These approaches are mutually exclusive. If you configure a new approach to obtain an IP address , the old IP address will be overwritten.

For details on how to obtain IP addresses through DHCP, see the “DHCP” chapter. The following describes the other three approaches for obtaining IP addresses.

Configuring the IP Address for an Interface

A device can receive and send IP packets only after the device is configured with an IP address. Only the interface configured with an IP address can run the IP protocol.

Configuring Multiple IP Addresses for an Interface

FS products support multiple IP address configuration on one interface, of which one is a primary IP address and the others are secondary IP addresses or slave addresses. Theoretically, the number of secondary IP addresses is not limited. However, secondary IP addresses

must belong to different networks and secondary IP addresses must be in different networks from primary IP addresses. In network construction, secondary IP addresses are often used in the following circumstances:

- A network does not have enough host addresses. For example, a LAN now needs one class C network to allocate 254 addresses. However, when the number of hosts exceeds 254, one class C network is not enough and another class C network is needed. In this case, two networks need to be connected. Therefore, more IP addresses are needed.
- Many old networks are based on L2 bridged networks without subnetting. You can use secondary IP addresses to upgrade the network to a routing network based on IP layer. For each subnet, one device is configured with one IP address.
- When two subnets of one network are isolated by another network, you can connect the isolated subnets by creating a subnet of the isolated network and configuring a secondary address. One subnet cannot be configured on two or more interfaces of a device.
- Slave IP addresses are used on gateway clusters. Slave IP addresses can be configured only after primary IP addresses are configured. Both slave IP addresses and primary IP addresses are configured based on L3 interfaces as mutual backup. Normally, master devices use primary IP addresses and slave devices use slave IP addresses. When a slave device is switched to a master device, the slave IP address becomes the primary IP address. When a master device is switched to a slave device, the primary IP address becomes the slave IP address.

Before configuring secondary IP addresses, make sure that primary IP addresses are configured. If one device in a network is configured with a secondary IP address, other devices must be configured with secondary IP addresses in the same network. If other devices are not configured with IP addresses, the secondary addresses can be set to primary IP addresses.

Before configuring slave IP addresses, make sure that primary IP addresses are configured. Slave IP addresses and primary IP addresses are mutual backup. Primary addresses are valid on master devices, and slave addresses are valid on slave devices. At any time, only one address is valid on an interface.

Slave IP addresses and primary IP addresses are mutual backup (Only one of them is valid on an interface). During DHCP deployment, slave IP addresses should be taken into consideration. For example, do not assign slave IP addresses. Otherwise, an address conflict may occur.

Configuring a MGMT IP Address and Gateway

This command is supported on L2 devices only.

L2 switch can be configured with a management IP address and gateway. Users can remotely manage L2 switches through telnet and need to modify the management IP address and default gateway of a L2 switch.

Obtaining an IP Addresses through PPP Negotiation

This command is supported on point-to-point interfaces only.

Through this configuration, a point-to-point interface accepts the IP address assigned by the peer end through PPP negotiation.

Borrowing an IP Addresses from Another Interface

One interface may not be configured with an IP address. To enable the interface, it must borrow an IP address from another interface.

IP addresses of Ethernet interfaces, tunnel interfaces, and loopback interfaces can be borrowed. However, these interfaces cannot borrow IP addresses from other interfaces.

The IP addresses of borrowed interfaces cannot be borrowed from other interfaces.

If a borrowed interface has multiple IP addresses, only the primary IP address can be borrowed.

The IP address of one interface can be lent to multiple interfaces.

IP addresses of borrowing interfaces are always consistent with and vary with IP addresses of borrowed interfaces.

Related Configuration

Configuring an Interface with One or More IP Addresses

- By default, an interface is not configured with an IP address.
- The **ip address** command is used to configure an IP address for an interface.
- After an IP address is configured, the IP address can be used for communication when it passes conflict detection.
- The **ip address** *ip-address mask* **secondary** command can be used to configure multiple secondary IP addresses.
- The **ip address** *ip-address mask***slave** command can be used to configure slave IP addresses.

Configuring an MGMT IP Address and Gateway

- In general, the **ip default-gateway** command is used to configure a default gateway for a L2 device and the **ip address** command is used to configure and manage the IP address of a VLAN.
- Users want to remotely manage L2 switches through telnet and modify the management IP addresses and default gateways of L2 switches. With the **ip address** command or the **ip default-gateway** command configured, the switches cannot access the devices since the configuration changes. In this case, you can use the **gateway** key word in the **ip address** command to modify the management IP addresses and default gateways.

Obtaining an IP Address through PPP Negotiation

- By default, the interface cannot obtain an IP address through PPP negotiation.
- The **ip address negotiate** command is used to configure IP address negotiation on a point-to-point interface.

Borrowing an IP Address from Other Interfaces

- By default, an interface is not configured with an IP address.
- The **ip unnumbered** command can be used to borrow IP addresses from other interfaces.

1.3.2 Broadcast Packet Processing

Working Principle

Broadcast is divided into two types. One is limited broadcast, and the IP address is 255.255.255.255. Because the broadcast is prohibited by routers, the broadcast is called local network broadcast. The other is directed broadcast. All host bits are 1s, for example, 192.168.1.255/24. The broadcast packets with these IP addresses can be forwarded.

If IP network devices forward limited broadcast packets (destination IP address is 255.255.255.255), the network may be overloaded, which severely affects network performance. This circumstance is called broadcast storm. Devices provide some approaches to confine broadcast storms within the local network and prevent continuous spread of broadcast storms. L2 network devices such as bridges and switches forward and spread broadcast storms.

The best way to avoid broadcast storm is to assign a broadcast address to each network, which is directed broadcast. This requires the IP protocol to use directed broadcast rather than limited broadcast to spread data.

For details about broadcast storms, see RFC 919 and RFC 922.

Directed broadcast packets refer to the broadcast packets destined for a subnet. For example, packets whose destination address is 172.16.16.255 are called directed broadcast packets. However, the node that generates the packets is not a member of the destination subnet.

After receiving directed broadcast packets, the devices not directly connected to the destination subnet forward the packets. After directed broadcast packets reach the devices directly connected to the subnet, the devices convert directed broadcast packets to limited broadcast packets (destination IP address is 255.255.255.255) and broadcast the packets to all hosts on the destination subnet at the link layer.

Related Configuration

Configuring an IP Broadcast Address

- By default, the IP broadcast address of an interface is 255.255.255.255.
- To define broadcast packets of other addresses, run the **ip broadcast-address** command on the interface.

Forwarding Directed Broadcast Packets

- By default, directed broadcast packets cannot be forwarded.
- On the specified interface, you can run the **ip directed-broadcast** command to enable directed broadcast packets forwarding. In this way, the interface can forward directed broadcast packets to networks that are directly connected. Broadcast packets can be transmitted within the destination subnet without affecting forwarding of other directed broadcast packets.
- On an interface, you can define an Access Control List (ACL) to transmit certain directed broadcast packets. After an ACL is defined, only directed broadcast packets that match the ACL are forwarded.

1.3.3 Sending ICMP Packets

Working Principle

ICMP Protocol Unreachable Message

A device receives non-broadcast packets destined for itself, and he packets contain the IP protocol that cannot be processed by the device. The device sends an ICMP protocol unreachable message to the source host. Besides, if the device does not know a route to forward packets, it also sends an ICMP host unreachable message.

ICMP Redirection Message

Sometimes, a route may be less than optimal, which makes a device send packets from the interface that receives packets. If a device sends packets from an interface on which it receives the packets, the device sends an ICMP redirection message to the source, informing the source that the gateway is another device on the same subnet. In this way, the source sends subsequent packets according to the optimal path.

ICMP Mask Response Message

Sometimes, a network device sends an ICMP mask request message to obtain the mask of a subnet.. The network device that receives the ICMP mask request message sends a mask response message.

Related Configuration

Enabling ICMP Protocol Unreachable Message

- By default, the ICMP Protocol unreachable message function is enabled on an interface.
- You can run the [**no**] **ip unreachables** command to disable or enable the function.

Enabling ICMP Redirection Message

- By default, the ICMP redirection message function is enabled on an interface.
- You can run the [**no**] **ip redirects** command to disable or enable the function.

Enabling ICMP Mask Response Message

- By default, the ICMP mask response message function is enabled on an interface.
- You can run the [**no**] **ip mask-reply** command to disable or enable the function.

1.3.4 Limiting Transmission Rate of ICMP Error Packets

Working Principle

This function limits the transmission rate of ICMP error packets to prevent DoS attacks by using the token bucket algorithm.

If an IP packet needs to be fragmented but the Don't Fragment (DF) bit in the header is set to 1, the device sends an ICMP destination unreachable packet (code 4) to the source host. This ICMP error packet is used to discover the path MTU. When there are too many other ICMP error packets, the ICMP destination unreachable packet (code 4) may not be sent. As a result, the path MTU discovery function fails. To avoid this problem, you should limit the transmission rate of ICMP destination unreachable packets and other ICMP error packets respectively.

Related Configuration

Configuring the Transmission Rate of ICMP Destination Unreachable Packets Triggered by DF Bit in the IP Header

- The default transmission rate is 10 packets every 100 milliseconds.
- The **ip icmp error-interval DF** command can be used to configure the transmission rate.

Configuring the Transmission Rate of Other ICMP Error Packets

- The default transmission rate is 10 packets every 100 milliseconds.
- The **ip icmp error-interval** command can be used to configure the transmission rate.

1.3.5 IP MTU

Working Principle

If an IP packet exceeds the IP MTU size, the FSOS software splits the packet. For all devices in the same physical network segment, the IP MTU of interconnected interfaces must be the same. You can adjust the link MTU of interfaces on FS products. After the link MTU of interfaces is changed, the IP MTU of interfaces will be changed. The IP MTU of interfaces automatically keeps consistent with the link MTU of interfaces. However, if the IP MTU of interfaces is adjusted, the link MTU of interfaces will not be changed.

Related Configuration

Setting the IP MTU

- By default, the IP MTU of an interface is 1500.

- The **ip mtu** command can be used to set the IP packet MTU.

1.3.6 IP TTL

Working Principle

An IP packet is transmitted from the source address to the destination address through routers. After a TTL value is set, the TTL value decreases by 1 every time when the IP packet passes a router. When the TTL value drops to zero, the router discards the packet. This prevents infinite transmission of useless packets and waste of bandwidth.

Related Configuration

Setting the IP TTL

- By default, the IP TTL of an interface is 64.
- The **ip ttl** command can be used to set the IP TTL of an interface.

1.3.7 IP Source Route

Working Principle

FS products support IP source routes. When a device receives an IP packet, it checks the options such as source route, loose source route, and record route in the IP packet header. These options are detailed in RFC 791. If the device detects that the packet enables one option, it responds; if the device detects an invalid option, it sends an ICMP parameter error message to the source and then discards the packet.

After the IP source route is enabled, the source route option is added to an IP packet to test the throughput of a specific network or help the packet bypasses the failed network. However, this may cause network attacks such as source address spoofing and IP spoofing.

Related Configuration

Configuring an IP Source Route

- By default, the IP source route function is enabled.
- The **ip source-route** command can be used to enable or disable the function.

1.3.8 IP Address Pool

Working Principle

A point-to-point interface can assign an IP address to the peer end through PPP negotiation. During PPP negotiation, the server checks authentication information of the client. If the client passes the authentication, the server assigns an IP address to the client (if the client is configured with an IP address and the IP address meets requirements of the server, the server approves the IP address of the client). The IP address of the peer end can be directly specified or assigned from the address pool.

Related Configuration

Enabling the Address Pool Function

- By default, the address pool function is enabled.
- The **ip address-pool local** command can be used to enable or disable the function.

Creating an Address Pool

- By default, no IP address pool is configured.
- The **ip local pool** command can be used to create or delete an address pool.

Assigning an IP Address to the Peer End through PPP Negotiation

- By default, an interface does not assign an IP address to the peer end.
- The **peer default ip address** command can be used to assign an IP address to the peer end.

1.4 Configuration

Configuration	Description and Command	
Configuring the IP Addresses of an Interface	(Mandatory) It is used to configure an IP address and allow the IP protocol to run on an interface.	
	ip address	Manually configures the IP address of an interface.
	ip address negotiate	Obtains the IP address of an interface through PPP negotiation.
	ip unnumbered	Borrows an IP address from another interface.
	ap-interface bvi *num* **ip address**	Configures the IP address of a BVI interface on an AP through AC.
Configuring Broadcast Forwarding	(Optional) It is used to set an IP broadcast address and enable directed broadcast forwarding.	
	ip broadcast-address	Configures an IP broadcast address.
	ip directed-broadcast	Enables directed broadcast forwarding.
Configuring ICMP Forwarding	(Optional) It is used to enable ICMP packet forwarding.	
	ip unreachables	Enables ICMP unreachable messages and host unreachable messages.
	ip redirects	Enables ICMP redirection messages.
	ip mask-reply	Enables ICMP mask response messages.
Configuring the Transmission Rate of ICMP Error Packets	Optional.	
	ip icmp error-interval DF	Configures the transmission rate of ICMP destination unreachable packets triggered by the DF bit in the IP header.
	ip icmp error-interval	Configures the transmission rate of ICMP error packets and ICMP redirection packets.
Setting the IP MTU	(Optional) It is used to configure the IP MTU on an interface.	
	ip mtu	Sets the MTU value.
Setting the IP TTL	(Optional) It is used to configure the TTL of unicast packets and broadcast packets.	
	ip ttl	Sets the TTL value.

Configuration	Description and Command	
Configuring an IP Source Route	(Optional) It is used to check the source routes.	
	ip source-route	Enables the IP source route function.

1.4.1 Configuring the IP Addresses of an Interface

Configuration Effect

Configure the IP address of an interface for communication.

Notes

- N/A

Configuration Steps

Configuring the IP Address of an Interface

- Mandatory
- Perform the configuration in L3 interface configuration mode.

Obtaining the IP Address of an Interface through PPP Negotiation

- Optional
- If a point-to-point interface is not configured with an IP address, obtain an IP address through PPP negotiation.
- Perform the configuration in L3 interface configuration mode.

Borrowing an IP Address from Another Interface

- Optional
- If a point-to-point interface is not configured with an IP address, borrow an IP address from another interface.
- Perform the configuration in L3 interface configuration mode.

Verification

Run the **show ip interface** command to check whether the configuration takes effect.

Related Commands

Manually Configuring the IP Address of an Interface

Command	**ip address** *ip-address network-mask* [**secondary**] | [**slave**]
Parameter Description	*ip-address*: 32-bit IP address, with 8 bits for each group. The IP address is expressed in decimal and groups are separated by a full stop (.). *network-mask*: 32-bit network mask. Value 1 indicates the mask bit and 0 indicates the host bit. Every 8 bits form one group. The network mask is expressed in decimal and groups are separated by a full stop (.). **secondary**: Secondary IP address. **slave**: Slave IP address.

Command Mode	Interface configuration mode
Usage Guide	N/A

Obtaining an IP Address of an Interface through PPP Negotiation

Command	**ip address negotiate**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Only point-to-point interfaces support obtaining IP addresses through PPP negotiation. After the **ip address negotiate** command is run on an interface, run the **peer default ip address** command at the peer end.

Borrowing an IP Addresses from Another Interface

Command	**ip unnumbered** *interface-type interface-number*
Parameter Description	*interface-type*: Interface type. *interface-number*: Interface ID.
Command Mode	Interface configuration mode
Usage Guide	An unnumbered interface indicates that the interface is enabled with the IP protocol without an IP address assigned. An unnumbered interface needs to be associated with an interface configured with an IP address. For an IP packet generated on an unnumbered interface, the source IP address of the packet is the IP address of the associated interface. In addition, the routing protocol process decides whether to send a route update packet to the unnumbered interface according to its associated IP address. If you want to use an unnumbered interface, pay attention to the following limitations: An Ethernet interface cannot be set to an unnumbered interface. When a serial interface encapsulates SLIP, HDLC, PPP, LAPB, and Frame-Relay, the serial interface can be set to an unnumbered interface. During Frame -Relay encapsulation, however, only a point-to-point interface can be configured as an unnumbered interface. AnX.25 interface cannot be configured as an unnumbered interface. The **ping** command cannot be used to check whether an unnumbered interface is working properly because an unnumbered interface is not configured with an IP address. However, you can monitor the status of an unnumbered interface remotely through SNMP. A device cannot be cold started through an unnumbered interface.

Configuration Example

Configuring an IP Address for an Interface

Configuration Steps	Configure IP address 192.168.23.110 255.255.255.0 on interface GigabitEthernet 0/0.
	FS#configure terminal FS(config)#interface gigabitEthernet 0/0

	FS(config-if-GigabitEthernet 0/0)# no switchport FS(config-if-GigabitEthernet 0/0)#ip address 192.168.23.110 255.255.255.0
Verification	Run the **show ip interface** command to check whether the configuration takes effect.
	FS# show ip interface gigabitEthernet 0/0 GigabitEthernet 0/0 IP interface state is: UP IP interface type is: BROADCAST IP interface MTU is: 1500 IP address is: 192.168.23.110/24 (primary)

Configuring a Slave IP Address for an Interface

Configuration Steps	Configure primary IP address 192.168.23.110 255.255.255.0 and slave IP address 192.168.24.110 255.255.255.0 on interface GigabitEthernet 0/0.
	FS#configure terminal FS(config)#interface gigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)# no switchport FS(config-if-GigabitEthernet 0/0)#ip address 192.168.23.110 255.255.255.0 FS(config-if-GigabitEthernet 0/0)#ip address 192.168.24.110 255.255.255.0 slave
Verification	Run the **show running-config interface** command to check whether the configuration takes effect.
	FS# show running-config interface gigabitEthernet 0/0 interface GigabitEthernet 0/0 ip address 192.168.23.110 255.255.255.0 ip address 192.168.24.110 255.255.255.0 slave

Obtaining an IP Address on a Point-to-point Interface through PPP Negotiation

Configuration Steps	Obtain an IP address on a point-to-point interface through negotiation.
	FS(config)#int virtual-ppp 1 FS(config-if-Virtual-ppp 1)#ip address negotiate
Verification	Run the **show run** command to check whether the configuration takes effect.
	FS#show run interface virtual-ppp 1 Building configuration...

	Current configuration: 48 bytes interface Virtual-ppp 1 ip address negotiate

1.4.2 Configuring Broadcast Forwarding

Configuration Effect

Set the broadcast address of an interface to 0.0.0.0 and enable directed broadcast forwarding.

Notes

N/A

Configuration Steps

Configuring an IP Broadcast Address

- (Optional) Some old hosts may identify broadcast address 0.0.0.0 only. In this case, set the broadcast address of the target interface to 0.0.0.0.
- Perform the configuration in L3 interface configuration mode.

Enabling Directed Broadcast Forwarding

- (Optional) If you want to enable a host to send broadcast packets to all hosts in a domain that it is not in, enable directed broadcast forwarding.
- Perform the configuration in L3 interface configuration mode.

Verification

Run the **show running-config interface** command to check whether the configuration takes effect.

Related Commands

Configuring an IP Broadcast Address

Command	**ip broadcast-address** *ip-address*
Parameter Description	*ip-address*: Broadcast address of an IP network.
Command Mode	Interface configuration mode
Usage Guide	Generally, the destination address of IP broadcast packets is all 1s, which is expressed as 255.255.255.255. The FSOS software can generate broadcast packets of other IP addresses through definition and receive self-defined broadcast packets and the broadcast packets with address 255.255.255.255.

Allowing Forwarding of Directed Broadcast Packets

Command	**ip directed-broadcast** [*access-list-number*]

Parameter Description	*access-list-number*: Access list number, ranging from 1 to 199 and from1300 to 2699. After an ACL is defined, only directed broadcast packets that match the ACL are forwarded.
Command Mode	Interface configuration mode
Usage Guide	If the **no ip directed-broadcast** command is run on an interface, the FSOS software will discard directed broadcast packets received from the network that is directly connected.

Configuration Example

Configuration Steps	On interface gigabitEthernet 0/1, set the destination address of IP broadcast packets to 0.0.0.0 and enable directed broadcast forwarding. FS#configure terminal FS(config)#interface gigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# no switchport FS(config-if-GigabitEthernet 0/1)#ip broadcast-address 0.0.0.0 FS(config-if-GigabitEthernet 0/1)#ip directed-broadcast
Verification	Run the **show ip interface** command to check whether the configuration takes effect. FS#show running-config interface gigabitEthernet 0/1 ip directed-broadcast ip broadcast-address 0.0.0.0

1.4.3 Configuring ICMP Forwarding

Configuration Effect

Enable ICMP unreachable messages, ICMP redirection messages, and mask response messages on an interface.

Notes

N/A

Configuration Steps

Enabling ICMP Unreachable Messages

- By default, ICMP unreachable messages are enabled.
- Optional)The **no ip unreachables** command can be used to disable ICMP unreachable messages.
- Perform the configuration in L3 interface configuration mode.

Enabling ICMP Redirection Messages

- By default, ICMP redirection messages are enabled.
- Optional)The **no ip redirects** command can be used to disable ICMP redirection messages.
- Perform the configuration in L3 interface configuration mode.

Enabling ICMP Mask Response Messages

- By default, ICMP mask response messages are enabled.
- Optional)The **no ip mask-reply** command can be used to disable ICMP mask response messages.
- Perform the configuration in L3 interface configuration mode.

Verification

Run the **show ip interface** command to check whether the configuration takes effect.

Related Commands

Enabling ICMP Unreachable Messages

Command	**ip unreachables**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Enabling ICMP Redirection Messages

Command	**ip redirects**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Enabling ICMP Mask Response Messages

Command	**ip mask-reply**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuration Steps	Enable ICMP unreachable messages, ICMP redirection messages, and mask response messages on interface gigabitEthernet 0/1.
	FS#configure terminal FS(config)#interface gigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# no switchport FS(config-if-GigabitEthernet 0/1)# ip unreachables FS(config-if-GigabitEthernet 0/1)# ip redirects FS(config-if-GigabitEthernet 0/1)# ip mask-reply

Verification	Run the **show ip interface** command to check whether the configuration takes effect.
	FS#show ip interface gigabitEthernet 0/1 GigabitEthernet 0/1 ICMP mask reply is: ON Send ICMP redirect is: ON Send ICMP unreachabled is: ON

1.4.4 Configuring the Transmission Rate of ICMP Error Packets

Configuration Effect

Configure the transmission rate of ICMP error packets.

Notes

N/A

Configuration Steps

Configuring the Transmission Rate of ICMP Destination Unreachable Packets Triggered by the DF Bit in the IP Header

- Optional
- Perform the configuration in global configuration mode.

Configuring the Transmission Rate of Other ICMP Error Packets

- Optional
- Perform the configuration in global configuration mode.

Verification

Run the **show running-config** command to check whether the configuration takes effect.

Related Commands

Configuring the Transmission Rate of ICMP Destination Unreachable Packets Triggered by the DF Bit in the IP Header

Command	**ip icmp error-interval DF** *milliseconds* [*bucket-size*]
Parameter Description	*milliseconds*: Refresh cycle of a token bucket. The value range is from 0 to 2,147,483,647 and the default value is 100 milliseconds. When the value is 0, the transmission rate of ICMP error packets is not limited. *bucket-size*: Number of tokens contained in a token bucket. The value range is from 1 to 200 and the default value is 10.
Command Mode	Global configuration mode.
Usage Guide	This function limits the transmission rate of ICMP error packets to prevent DoS attacks by using the token bucket algorithm. If an IP packet needs to be fragmented but the DF bit in the header is set to 1, the device sends an ICMP destination unreachable packet (code 4) to the source host. This ICMP error packet is used to discover the path MTU. When there are too many other ICMP error packets, the ICMP destination unreachable packet (code 4) may not be sent. As a result, the

	path MTU discovery function fails. To avoid this problem, you should limit the transmission rate of ICMP destination unreachable packets and other ICMP error packets respectively. It is recommended to set the refresh cycle to integral multiples of 10 milliseconds. If the refresh cycle is set to a value greater than 0 and smaller than 10 milliseconds, the refresh cycle that actually takes effect is 10 milliseconds. For example, if the refresh rate is set to 1 per 5 milliseconds, the refresh rate that actually takes effect is 2 per 10 milliseconds. If the refresh cycle is not integral multiples of 10 milliseconds, the refresh cycle that actually takes effect is automatically converted to integral multiples of 10 milliseconds. For example, if the refresh rate is set to 3 per 15 milliseconds, the refresh rate that actually takes effect is 2 per 10milliseconds.

Configuring the Transmission Rate of Other ICMP Error Packets

Command	**ip icmp error-interval** *milliseconds* [*bucket-size*]
Parameter Description	*milliseconds*: Refresh cycle of a token bucket. The value range is 0to 2,147,483,647, and the default value is **100** (ms). When the value is **0**, the transmission rate of ICMP error packets is not limited. *bucket-size*: Number of tokens contained in a token bucket. The value range is 1to 200 and the default value is **10**.
Command Mode	Global configuration mode.
Usage Guide	This function limits the transmission rate of ICMP error packets to prevent DoS attacks by using the token bucket algorithm. It is recommended to set the refresh cycle to integral multiples of 10 milliseconds. If the refresh cycle is set to a value greater than 0 and smaller than 10 milliseconds, the refresh cycle that actually takes effect is 10 milliseconds. For example, if the refresh rate is set to 1 per 5 milliseconds, the refresh rate that actually takes effect is 2 per 10 milliseconds. If the refresh cycle is not integral multiples of 10 milliseconds, the refresh cycle that actually takes effect is automatically converted to integral multiples of 10 milliseconds. For example, if the refresh rate is set to 3 per 15 milliseconds, the refresh rate that actually takes effect is 2 per 10 milliseconds.

Configuration Example

Configuration Steps	Set the transmission rate of ICMP destination unreachable packets triggered the DF bit in IP header to 100 packets per second and the transmission rate of other ICMP error packets to 10 packets per second.
	FS(config)# ip icmp error-interval DF 1000 100 FS(config)# ip icmp error-interval 1000 10
Verification	Run the **show running-config** command to check whether the configuration takes effect.
	FS#show running-config | include ip icmp error-interval ip icmp error-interval 1000 10 ip icmp error-interval DF 1000 100

1.4.5 Setting the IP MTU

Configuration Effect

Adjust the IP packet MTU.

Notes

N/A

Configuration Steps

- (Optional) When the IP MTU of interconnected interfaces is different on devices in the same physical network segment, set the IP MTU to the same value.
- Perform the configuration in L3 interface configuration mode.

Verification

Run the **show ip interface** command to check whether the configuration takes effect.

Related Commands

Setting the IP MTU

Command	**ip mtu***bytes*
Parameter Description	*bytes*: IP packet MTU. The value range is from 68 to 1,500 bytes.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuration Steps	Set the IP MTU of interface gigabitEthernet 0/1 to 512 bytes.
	FS#configure terminal FS(config)#interface gigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# no switchport FS(config-if-GigabitEthernet 0/1)#ip mtu 512
Verification	Run the **show ip interface** command to check whether the configuration takes effect.
	FS# show ip interface gigabitEthernet 0/1 IP interface MTU is: 512

1.4.6 Setting the IP TTL

Configuration Effect

Modify the IP TTL value of an interface.

Notes

N/A

Configuration Steps

- Optional

- Perform the configuration in L3 interface configuration mode.

Verification

Run the **show run-config** command to check whether the configuration takes effect.

Related Commands

Setting the IP TTL

Command	**ip ttl** *value*
Parameter Description	*value*: TTL value. The value range is from 0 to 255.
Command Mode	Global configuration mode.
Usage Guide	N/A

Configuration Example

Configuration Steps	• Set the TTL of unicast packets to 100.
	FS#configure terminal FS(config)#ip ttl 100
Verification	Run the **show run-config** command to check whether the configuration takes effect.
	FS#show running-config ip ttl 100

1.4.7 Configuring an IP Source Route

Configuration Effect

Enable or disable the IP source route function.

Notes

N/A

Configuration Steps

- By default, the IP source route function is enabled.
- Optional) The **no ip source-route** command can be used to disable the IP source route function.

Verification

Run the **show run-config** command to check whether the configuration takes effect.

Related Commands

Configuring an IP Source Route

Command	**ip source-route**
Parameter Description	N/A
Command Mode	Global configuration mode.
Usage Guide	N/A

Configuration Example

Configuration Steps	● Disable the IP source route function.
	FS#configure terminal FS(config)#no ip source-route
Verification	Run the **show run-config** command to check whether the configuration takes effect.
	FS#show running-config no ip source-route

1.4.8 Configuring an IP Address Pool

Configuration Effect

Assign an IP address to a client through PPP negotiation.

Notes

N/A

Configuration Steps

Enabling the IP Address Pool Function

- Optional
- Perform the configuration in global configuration mode.

Creating an IP Address Pool

- Optional
- An IP address pool can be created only after the IP address pool function is enabled. After the IP address pool function is disabled, the created address pool is automatically deleted.
- Perform the configuration in global configuration mode.

Assigning an IP Address to the Peer End through PPP Negotiation

- Optional
- Perform the configuration in L3 interface configuration mode.

Verification

Run the **show run-config** command to check whether the configuration takes effect.

Related Commands

Enabling the IP Address Pool Function

Command	**ip address-pool local**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, the IP address pool function is enabled. You can configure an IP address pool to assign an IP address to the peer end through PPP negotiation. To disable the IP address pool function, run the **no ip address-pool local** command. All IP address pools configured previously will be deleted.

Creating an IP Address Pool

Command	**ip local pool** *pool-namelow-ip-address*[*high-ip-address*]
Parameter Description	*pool-name*: Name of a local IP address pool. **default** indicates the default address pool name. *low-ip-address*: Smallest IP address in an IP address pool. *high-ip-address*: Optional)Largest IP address in an IP address pool. If the largest IP address is not specified, the IP address pool contains only one IP address, that is, *low-ip-address*.
Command Mode	Global configuration mode
Usage Guide	The command is used to create one or more IP address pools to assign IP addresses to peer ends through PPP negotiation.

Assigning an IP Address to the Peer End through PPP Negotiation

Command	**peer default ip address** {*ip-address* | **pool** [*pool-name*] }
Parameter Description	*ip-address*: IP address assigned to the peer end. *pool-name*: (Optional) Specifies the address pool that assigns IP addresses. If this parameter is not set, IP addresses are assigned from the default address pool.
Command Mode	Interface configuration mode
Usage Guide	If the peer end is not configured with an IP address while the local device is configured with an IP address, you can enable the local device to assign an IP address to the peer end. Run the **ip address negotiate** command on the peer end and the **peer default ip address** command on the local device so that the peer end can accept the IP address assigned through PPP negotiation. The **peer default ip address** command can be configured on only PPP or SLIP interfaces. The **peer default ip address pool** command is used to assign an IP address to the peer end from an IP address pool. The IP address pool is configured through the **ip local pool** command. The **peer default ip address** *ip-address* command is used to specify an IP address for the peer end. The command cannot be run on virtual template interfaces or asynchronous interfaces.

Configuration Example

Configuration Steps	● Assign an IP address from address pool “quark” to the peer end on interface “dialer1”.

	FS#configure terminal FS(config)# ip address-pool local FS(config)# ip local pool quark 172.16.23.2 172.16.23.255 FS(config)# interface dialer 1 FS(config-if-dialer 1)#peer default ip address pool quark
Verification	Run the **show run-config** command to check whether the configuration takes effect.
	FS#show running-config ip local pool quark 172.16.23.2 172.16.23.255 ! interface dialer 1 peer default ip address pool quark

1.5 Monitoring

Displaying

Description	Command
Displays the IP address of an interface.	**show ip interface** [*interface-typeinterface-number* / **brief**]
Displays IP packet statistics.	**show ip packet statistics** [**total** | *interface-name*]
Displays statistics on sent and received IP packets in the protocol stack.	**show ip packet queue**
Displays address pool statistics.	**show ip pool** [*pool-name*]

2 Configuring ARP

2.1 Overview

In a local area network (LAN), each IP network device has two addresses: 1) local address. Since the local address is contained in the header of the data link layer (DLL) frame, it is a DLL address. However, it is processed by the MAC sublayer at the DLL and thereby is usually called the MAC address. MAC addresses represent IP network devices on LANs. 2) network address. Network addresses on the Internet represent IP network devices and also indicate the networks where the devices reside.

In a LAN, two IP devices can communicate with each other only after they learn the 48-bit MAC address of each other. The process of obtaining the MAC address based on the IP address is called address resolution. There are two types of address resolution protocols: 1) Address Resolution Protocol (ARP); 2) Proxy ARP. ARP and Proxy ARP are described respectively in RFC 826 and RFC 1027.

ARP is used to bind the MAC address with the IP address. When you enter an IP address, you can learn the corresponding MAC address through ARP. Once the MAC address is obtained, the IP-MAC mapping will be saved to the ARP cache of the network device. With the MAC address, the IP device can encapsulate DLL frames and send them to the LAN. By default, IP and ARP packets on the Ethernet are encapsulated in Ethernet II frames.

Protocols and Standards

- RFC 826: An Ethernet Address Resolution Protocol
- RFC 1027: Using ARP to implement transparent subnet gateways

2.2 Applications

Application	Description
LAN-based ARP	A user learns the MAC addresses of other users in the same network segment through ARP.
Proxy ARP-based Transparent Transmission	With Proxy ARP, a user can directly communicate with users in another network without knowing that it exists.

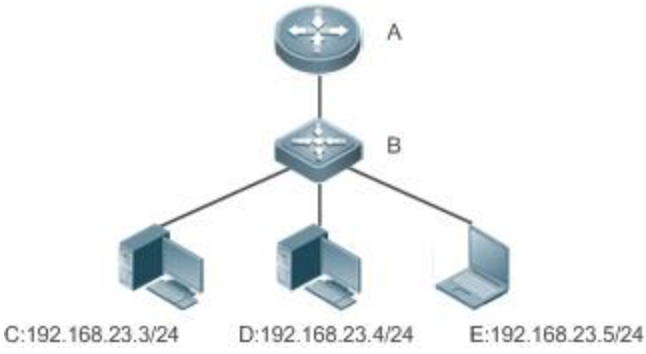
2.2.1 LAN-based ARP

Scenario

ARP is required in all IPv4 LANs.

- A user needs to learn the MAC addresses of other users through ARP to communicate with them.

Figure 2- 1



Remarks	A is a router. B is a switch. It acts as the gateway. C, D, and E are hosts.

Deployment

- Enable ARP in a LAN to implement IP-MAC mapping.

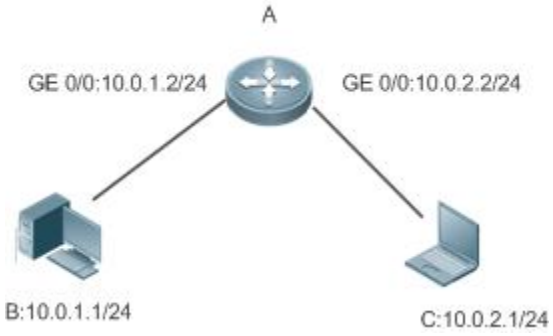
2.2.2 Proxy ARP-based Transparent Transmission

Scenario

Transparent transmission across IPv4 LANs is performed.

- Enable Proxy ARP on the router to achieve direct communication between users in different network segments.

Figure 2- 2



Remarks	A is a router connecting two LANs. B and C are hosts in different subnets. No default gateway is configured for them.

Deployment

- Enable Proxy ARP on the subnet gateway. After configuration, the gateway can act as a proxy to enable a host without any route information to obtain MAC addresses of IP users in other subnets.

2.3 Features

Overview

Feature	Description
Static ARP	Users can manually specify IP-MAC mapping to prevent the device from learning incorrect ARP entries.
ARP Attributes	Users can specify the ARP entry timeout, ARP request retransmission times and interval, and maximum number of unresolved ARP entries.
Trusted ARP	Trusted ARP is used to prevent ARP spoofing.
Gratuitous ARP	Gratuitous ARP is used to detect IP address conflicts and enable peripheral devices to update ARP entries.
Proxy ARP	A proxy replies to the ARP requests from other devices in different subnets.
Any IP ARP	Users can access the network without changing the IP address and gateway.

ARP Trustworthiness Detection	Neighbor Unreachable Detection (NUD) is used to ensure that correct ARP entries are learned.
Disabling Dynamic ARP Entry Learning	After dynamic ARP learning is disabled on an interface, the interface does not learn dynamic ARP entries.
ARP Scanning	Neighbors in LANs are scanned.
ARP Tracking	Enable ARP tracking. When a tracked object is unreachable, the device deletes the corresponding ARP entry.

2.3.1 Static ARP

Static ARP entries can be configured manually or assigned by the authentication server. The manually configured ones prevail. Static ARP can prevent the device from learning incorrect ARP entries.

Working Principle

If static ARP entries are configured, the device does not actively update ARP entries and these ARP entries permanently exist.

When the device forwards Layer-3 packets, the static MAC address is encapsulated in the Ethernet header as the destination MAC address.

Related Configuration

- Enabling Static ARP

Run the **arp** *ip-address mac-address type* command in global configuration mode to configure static ARP entries. By default, no static ARP entry is configured.. ARP encapsulation supports only the Ethernet II type, which is represented by ARPA.ARP Attributes

2.3.2 ARP attribute

Users can specify the ARP timeout, ARP request retransmission interval and times, maximum number of unresolved ARP entries, and maximum number of ARP entries on an interface.

Working Principle

- ARP Timeout

The ARP timeout only applies to the dynamically learned IP-MAC mapping. When the ARP entry timeout expires, the device sends a unicast ARP request packet to detect whether the peer end is online. If it receives an ARP reply from the peer end, it does not delete this ARP entry. Otherwise, the device deletes this ARP entry.

When the ARP timeout is set to a smaller value, the mapping table stored in the ARP cache is more accurate but ARP consumes more network bandwidth.

- ARP Request Retransmission Interval and Times

The device consecutively sends ARP requests to resolve an IP address to a MAC address. The shorter the retransmission interval is, the faster the resolution is. The more times the ARP request is retransmitted, the more likely the resolution will succeed and the more bandwidth ARP will consume.

- Maximum Number of Unresolved ARP Entries

In a LAN, ARP attacks and scanning may cause a large number of unresolved ARP entries generated on the gateway. As a result, the gateway fails to learn the MAC addresses of the users. To prevent such attacks, users can configure the maximum number of unresolved ARP entries.

Maximum Number of ARP Entries on an Interface

Configure the maximum number of ARP entries on a specified interface to prevent ARP entry resource waste.

Related Configuration

Configuring the ARP Timeout

Run the **arp timeout** *seconds* command in interface configuration mode to configure the ARP timeout. The default timeout is 3,600 seconds. You can change it based on actual situations.

Configuring the ARP Request Retransmission Interval and Times

- Run the **arp retry interval** *seconds* command in global configuration mode to configure the ARP request retransmission interval. The default interval is 1 second. You can change it based on actual situations.
- Run the **arp retry times** *number* command in global configuration mode to configure the ARP request retransmission times. The default number of retransmission times is 5. You can change it based on actual situations.

Configuring the Maximum Number of Unresolved ARP Entries

Run the **arp unresolve** *number* command in global configuration mode to configure the maximum number of unresolved ARP entries. The default value is the maximum number of ARP entries supported by the device. You can change it based on actual situations.

Configuring the Maximum Number of ARP Entries on an Interface

Run the **arp cache interface-limit** *limit* command in interface configuration mode to configure the maximum number of ARP entries learned on an interface. The default number is 0. You can change it based on actual situations. This command also applies to static ARP entries.

2.3.3 Trusted ARP

Working Principle

As a type of special ARP entries, trusted ARP entries are added to the ARP table to prevent ARP spoofing. Trusted ARP entries have characteristics of both static and dynamic ARP entries, with a priority higher than that of dynamic ARP entries and lower than that of static ARP entries. Trusted ARP has an aging mechanism similar to that of dynamic ARP. When an ARP entry ages, the device actively sends an ARP request packet to detect whether the corresponding user exists. If the user sends a reply, the device regards the user active and updates the ARP timeout. Otherwise, the device deletes the ARP entry. Trusted ARP has characteristics of static ARP, that is, the device does not learn ARP packets to update the MAC address and interface ID in the ARP entry.

When a user goes online on a GSN client, the authentication server obtains the user's reliable IP-MAC mapping through the access switch, and adds trusted ARP entries to the user's gateway. This process is transparent to the network administrator and does not affect the administrator’s work on network management.

Since trusted ARP entries come from authentic sources and will not be updated, they can efficiently prevent ARP spoofing targeted at the gateway.

Related Configuration

Enabling Trusted ARP

- Run the **service trustedarp** command in global configuration mode to enable trusted ARP. This function is disabled by default.
- Run the **arp trusted user-vlan** *vid1* **translated-vlan** *vid2* command in global configuration mode to implement VLAN redirection. This function is disabled by default. If the VLAN pushed by the server differs from the VLAN in the trusted ARP entry, users need to enable VLAN redirection.
- Run the **arp trusted aging** command in global configuration mode to enable ARP aging. Trusted ARP entries are not aged by default.
- Run the **arp trusted number** command in global configuration mode to configure the capacity of trusted ARP entries. The default value is half of the total capacity of ARP entries. You can change it based on actual situations.

2.3.4 Gratuitous ARP

Working Principle

Gratuitous ARP packets are a special type of ARP packets. In a gratuitous ARP packet, the source and destination IP addresses are the IP address of the local device. Gratuitous ARP packets have two purposes:

7. IP address conflict detection. If the device receives a gratuitous packet and finds the IP address in the packet the same as its own IP address, it sends an ARP reply to notify the peer end of the IP address conflict.
8. ARP update. When the MAC address of an interface changes, the device sends a gratuitous ARP packet to notify other devices to update ARP entries.

The device can learn gratuitous ARP packets. After receiving a gratuitous ARP packet, the device checks whether the corresponding dynamic ARP entry exists. If yes, the device updates the ARP entry based on the information carried in the gratuitous ARP packet.

Related Configuration

Enabling Gratuitous ARP

Run the **arp gratuitous-send interval** *seconds* [*number*] command in interface configuration mode to enable gratuitous ARP. This function is disabled on interfaces by default. Generally you need to enable this function on the gateway interface to periodically update the MAC address of the gateway on the downlink devices, which prevents others from faking the gateway.

2.3.5 Proxy ARP

Working Principle

The device enabled with Proxy ARP can help a host without any route information to obtain MAC addresses of IP users in other subnets. For example, if the device receiving an ARP request finds the source IP address in a different network segment from the destination IP address and knows the route to the destination address, the device sends an ARP reply containing its own Ethernet MAC address. This is how Proxy ARP works.

Related Configuration

Enabling Proxy ARP

- Run the **ip proxy-arp** command in interface configuration mode to enable Proxy ARP.
- This function is enabled on routers while disabled on switches by default.

2.3.6 Any IP ARP

Working Principle

If any IP ARP is enabled, users can access the network with any IP address. This applies when a user is using his own laptop in a hotel and wants to access the network without changing the IP address and gateway. If the gateway receiving an ARP request finds the source IP address in a different subnet and the destination address possibly not its own address, the gateway still sends an ARP reply and creates a direct route for the user.

Related Configuration

Enabling Any IP ARP

Run the **arp any-ip** command in interface configuration mode to enable any IP ARP. This function is disabled on interfaces by default.

2.3.7 ARP Trustworthiness Detection

Working Principle

The **arp trust-monitor enable** command is used to enable anti-ARP spoofing to prevent excessive useless ARP entries from occupying device resources. After ARP trustworthiness detection is enabled on a Layer-3 interface, the device receives ARP request packets from this interface:

1. If the corresponding entry does not exist, the device creates a dynamic ARP entry and performs NUD after 1 to 5 seconds. That is, the device begins to age the newly learned ARP entry and sends a unicast ARP request. If the device receives an ARP update packet from the peer end within the aging time, it stores the entry. If not, it deletes the entry.
2. If the corresponding ARP entry exists, NUD is not performed.
3. If the MAC address in the existing dynamic ARP entry is updated, the device also performs NUD.

Since this function adds a strict confirmation procedure in the ARP learning process, it affects the efficiency of ARP learning.

After this function is disabled, NUD is not required for learning and updating ARP entries.

Related Configuration

Enabling ARP Trustworthiness Detection

Run the **arp trust-monitor enable** command in interface configuration mode to enable ARP trustworthiness detection. This function is disabled by default.

2.3.8 Disabling Dynamic ARP Entry Learning

Working Principle

After dynamic ARP entry learning is disabled on an interface, this interface does not learn dynamic ARP entries.

Related Configuration

Disabling Dynamic ARP Entry Learning

- Dynamic ARP entry learning is enabled on interfaces by default.
- Run the **no arp-learning enable** command in interface configuration mode to disable dynamic ARP entry learning.

2.3.9 ARP Scanning

Working Principle

After ARP scanning is enabled, the device scans the neighbors in a LAN to learn their ARP entries. The device scans the neighbors in the network segments from the primary IP address to secondary IP address on an interface or scans only the neighbors in the specified address range. ARP scanning takes effect when the Layer-3 interface is UP (that is, the link is UP and configured with an IP address). One ARP scanning configuration takes effect only once. It cannot be saved and loses effect the next time.

Related Configuration

Enabling ARP Scanning

Run the **arp scan** [*start-ip-address end-ip-address*] command in interface configuration mode to enable ARP scanning. This function is disabled by default.

2.4 Configuration

Configuration	Description and Command	
Enabling Static ARP	(Optional) It is used to enable static IP-MAC binding.	
	arp	Enables static ARP.
Configuring ARP Attributes	(Optional) It is used to specify the ARP timeout, ARP request retransmission interval and times, maximum number of unresolved ARP entries, and maximum number of ARP entries on an interface.	
	arp timeout	Configures the ARP timeout.
	arp retry interval	Configures the ARP request retransmission interval.
	arp unresolve	Configures the maximum number of unresolved ARP entries.
	arp cache interface-limit	Configures the maximum number of ARP entries on an interface.
Enabling Trusted ARP	(Optional) It is used to enable anti-ARP spoofing.	
	service trustedarp	Enables trusted ARP.
	arp trusted user-vlan	Enables VLAN redirection when a trusted ARP entry is added.
	arp trusted aging	Enables trusted ARP aging.
	arp trusted	Configures the capacity of trusted ARP entries.
Enabling Gratuitous ARP	(Optional) It is used to detect IP address conflicts and enables peripheral devices to update ARP entries.	
	arp gratuitous-send interval	Enables gratuitous ARP.
Enabling Proxy ARP	(Optional) It is used to act as a proxy to reply to ARP requests from the devices in different subnets.	

Configuration	Description and Command	
	ip proxy-arp	Enables Proxy ARP.
Enabling Local Proxy ARP	(Optional) It is used to act as a proxy to reply to ARP requests from other devices in the same subnet.	
	local-proxy-arp	Enables local Proxy ARP.
Enabling Any IP ARP	(Optional) It is used to allow users to access the network without changing the IP address and gateway.	
	arp any-ip	Enables any IP ARP.
Enabling ARP Trustworthiness Detection	(Optional) It is used to unicast ARP request packets to ensure that correct ARP entries are learned.	
	arp trusted-monitor enable	Enables ARP trustworthiness detection.
Disabling Dynamic ARP Learning	(Optional) It is used to disable dynamic ARP learning on an interface.	
	no arp-learning enable	Disables dynamic ARP learning on an interface.
Enabling ARP Scanning	(Optional) It is used to enable ARP scanning on an interface.	
	arp scan	Enables ARP scanning on an interface.
Enabling ARP Tracking	(Optional) It is used to delete the corresponding ARP entry when a tracked object is unreachable.	
	arp track	Enables ARP tracking so that the corresponding ARP entry is deleted when a tracked object becomes unreachable.

2.4.1 Enabling Static ARP

Configuration Effect

Users can manually specify IP-MAC mapping to prevent the device from learning incorrect ARP entries.

Notes

After a static ARP entry is configured, the Layer-3 switch learns the physical port corresponding to the MAC address in the static ARP entry before it performs Layer-3 routing.

Configuration Steps

Configuring Static ARP Entries

- Optional.
- You can configure a static ARP entry to bind the IP address of the uplink device with its MAC address to prevent MAC change caused by ARP attacks.
- Configure static ARP entries in global configuration mode.

Verification

Run the **show running-config** command to check whether the configuration takes effect. Or run the **show arp static** command to check whether a static ARP cache table is created.

Related Commands

Configuring Static ARP Entries

Command	**arp** *ip-address mac-address type*
Parameter Description	*ip-address*: Indicates the IP address mapped to a MAC address, which is in four-part dotted-decimal format. *mac-address*: Indicates the DLL address, consisting of 48 bits. *type*: Indicates the ARP encapsulation type. For an Ethernet interface, the keyword is **arpa**.
Command Mode	Global configuration mode
Usage Guide	The FSOS queries a 48-bit MAC address based on a 32-bit IP address in the ARP cache table. Since most hosts support dynamic ARP resolution, usually the static ARP mapping are not configured. Use the **clear arp-cache** command to delete the dynamic ARP entries.

Configuration Example

Scenario	For the network topology, see Figure 2- 1.
Configuration Steps	Configure a static ARP entry on B to statically bind the IP address of A with the MAC address. FS(config)#arp 192.168.23.1 00D0.F822.334B arpa
Verification	Run the **show arp static** command to display the static ARP entry. FS(config)#show arp static Protocol Address Age(min) Hardware Type Interface Internet 192.168.23.1 <static> 00D0.F822.334B arpa 1 static arp entries exist.

Common Errors

- The MAC address in static ARP is incorrect.

2.4.2 Configuring ARP Attributes

Configuration Effect

Users can specify the ARP timeout, ARP request retransmission interval and times, maximum number of unresolved ARP entries, and maximum number of ARP entries on an interface.

Configuration Steps

Configuring the ARP Timeout

- Optional.
- In a LAN, if a user goes online/offline frequently, it is recommended to set the ARP timeout small to delete invalid ARP entries as soon as possible.

- Configure the ARP timeout in interface configuration mode.

Configuring the ARP Request Retransmission Interval and Times

- Optional.
- If the network resources are insufficient, it is recommended to set the ARP request retransmission interval great and the retransmission times small to reduce the consumption of network bandwidths.
- Configure the ARP request retransmission interval and times in global configuration mode.

Configuring the Maximum Number of Unresolved ARP Entries

- Optional.
- If the network resources are insufficient, it is recommended to set the maximum number of unresolved ARP entries small to reduce the consumption of network bandwidths.
- Configure the maximum number of unresolved ARP entries in global configuration mode.

Configuring the Maximum Number of ARP Entries on an Interface

- Optional.
- Configure the maximum number of ARP entries on an interface in interface configuration mode.

Verification

Run the **show arp timeout** command to display the timeouts of all interfaces.

Run the **show running-config** command to display the ARP request retransmission interval and times, maximum number of unresolved ARP entries, and maximum number of ARP entries on an interface.

Related Commands

Configuring the ARP Timeout

Command	**arp timeout** *seconds*
Parameter Description	*seconds*: Indicates the timeout in seconds, ranging from 0 to 2,147,483. The default value is 3,600.
Command Mode	Interface configuration mode
Usage Guide	The ARP timeout only applies to the dynamically learned IP-MAC mapping. When the ARP timeout is set to a smaller value, the mapping table stored in the ARP cache is more accurate but ARP consumes more network bandwidth. Unless otherwise specified, do not configure the ARP timeout.

Configuring the ARP Request Retransmission Interval and Times

Command	**arp retry interval** *seconds*
Parameter Description	*seconds*: Indicates the ARP request retransmission interval in seconds, ranging from 1 to 3,600. The default value is 1.
Command Mode	Global configuration mode
Usage Guide	If a device frequently sends ARP requests, affecting network performance, you can set the ARP request retransmission interval longer. Ensure that this interval does not exceed the ARP timeout.

Configuring the Maximum Number of Unresolved ARP Entries

Command	**arp unresolve** *number*
Parameter Description	*number*: Indicates the maximum number of unresolved ARP entries, ranging from 1 to 8,192. The default value is 8,192.
Command Mode	Global configuration mode
Usage Guide	If a large number of unresolved entries exist in the ARP cache table and remain in the table after a while, it is recommended to use this command to limit the number of unresolved ARP entries.

Configuring the Maximum Number of ARP Entries on an Interface

Command	**arp cache interface-limit** *limit*
Parameter Description	*limit*: Indicates the maximum number of ARP entries that can be learned on an interface, including configured ARP entries and dynamically learned ARP entries. The value ranges from 0 to the ARP entry capacity supported by the device. 0 indicates no limit on this number.
Command Mode	Interface configuration mode
Usage Guide	Limiting the number of ARP entries on an interface can prevent malicious ARP attacks from generating excessive ARP entries on the device and occupying entry resources. The configured value must be equal to or greater than the number of the ARP entries learned by the interface. Otherwise, the configuration does not take effect. The configuration is subject to the ARP entry capacity supported by the device.

Configuration Example

Scenario	For the network topology, see Figure 2- 1.
Configuration Steps	● Set the ARP timeout to 60 seconds on port GigabitEthernet 0/1. ● Set the maximum number of learned ARP entries to 300 on port GigabitEthernet 0/1. ● Set the ARP request retransmission interval to 3 seconds. ● Set the ARP request retransmission times to 4. ● Set the maximum number of unresolved ARP entries to 4,096.
	FS(config)#interface gigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)#arp timeout 60 FS(config-if-GigabitEthernet 0/1)#arp cache interface-limit 300 FS(config-if-GigabitEthernet 0/1)#exit FS(config)#arp retry interval 3 FS(config)#arp retry times 4 FS(config)#arp unresolve 4096 FS(config)#arp dynamic-entry-limit 1 2 1000
Verification	● Run the **show arp timeout** command to display the timeout of the interface. ● Run the **show running-config** command to display the ARP request retransmission interval and times, maximum number of unresolved ARP entries, and maximum number of ARP entries on the interface.
	FS#show arp timeout

```
Interface                    arp timeout(sec)
----------------------   ----------------
GigabitEthernet 0/1        60
GigabitEthernet 0/2        3600
GigabitEthernet 0/4        3600
GigabitEthernet 0/5        3600
GigabitEthernet 0/7        3600
VLAN 100                   3600
VLAN 111                   3600
Mgmt 0                     3600

FS(config)# show running-config
arp unresolve 4096
arp retry times 4
arp retry interval 3
arp dynamic-entry-limit 1 2 1000
!
interface GigabitEthernet 0/1
 arp cache interface-limit 300
```

2.4.3 Enabling Trusted ARP

Configuration Effect

The gateway is protected from ARP spoofing.

Notes

Trusted ARP is supported only on switches.

Configuration Steps

- To deploy a GSN solution, enable trusted ARP.
- To deploy a GSN solution, enable trusted ARP.
- Enable trusted ARP in global configuration mode.

Verification

Run the **show arp trusted** command to display trusted ARP entries.

Run the **show running** command to check whether the configuration takes effect.

Related Commands

Enabling Trusted ARP

Command	**service trustedarp**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Trusted ARP is an anti-ARP spoofing function. As a part of the GSN solution, trusted ARP needs to be used with the GSN solution.

Enabling VLAN Redirection When a Trusted ARP Entry Is Added

Command	**arp trusted user-vlan** *vid1* **translated-vlan** *vid2*
Parameter Description	*vid1*: Indicates the VLAN ID configured on the server. *vid2*: Indicates the ID of the VLAN redirected.
Command Mode	Global configuration mode
Usage Guide	This command takes effect only after trusted ARP is enabled. Configure this command only when the VLAN pushed by the server differs from the VLAN in the trusted ARP entry.

Displaying Trusted ARP Entries

Command	**show arp trusted** [*ip* [*mask*]]
Parameter Description	*ip*: Indicates the IP address. The ARP entry of the specified IP address is displayed. If keyword **trusted** is specified, only the trusted ARP entries are displayed. Otherwise, the non-trusted ARP entries are displayed. *mask*: ARP entries within the IP subnet are displayed. If keyword **trusted** is specified, only the trusted ARP entries are displayed. Otherwise, the non-trusted ARP entries are displayed.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Deleting Trusted ARP Entries

Command	**clear arp trusted** [*ip* [*mask*]]
Parameter Description	*ip*: Indicates the IP address. The ARP entry of the specified IP address is displayed. If keyword **trusted** is specified, only the trusted ARP entries are displayed. Otherwise, the non-trusted ARP entries are displayed. *mask*: ARP entries within the IP subnet are displayed. If keyword **trusted** is specified, only the trusted ARP entries are displayed. Otherwise, the non-trusted ARP entries are displayed.
Command Mode	Privileged EXEC mode
Usage Guide	After you run the **clear arp trusted** command to delete all trusted ARP entries on the switch, users may fail to access the network. It is recommended to use the **clear arp trusted** *ip* command to delete a specified trusted ARP entry.

Enabling Trusted ARP Aging

Command	**arp trusted aging**

Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After you configure this command, trusted ARP entries begin to age, with the aging time the same as the dynamic ARP aging time. You can run the **arp timeout** command in interface configuration mode to configure the aging time.

Adjusting the Capacity of Trusted ARP Entries

Command	**arp trusted** *number*
Parameter Description	*number*: The minimum value is 10. The maximum number is the capacity supported by the device minus 1,024. By default, the maximum number of trusted ARP entries is half of the total capacity of ARP entries.
Command Mode	Privileged EXEC mode
Usage Guide	To make this command take effect, enable trusted ARP first. Trusted ARP entries and other entries share the memory. If trusted ARP entries occupy much space, dynamic ARP entries may not have sufficient space. Set the number of ARP entries based on the actual requirement. Do not set it to an excessively large value.

Configuration Example

Scenario	For the network topology, see Figure 2- 1.
Configuration Steps	● Enable trusted ARP. ● Enable VLAN redirection. ● Enable trusted ARP aging. ● Set the maximum number of trusted ARP entries to 1,024.
	FS(config)#servicetrustedarp FS(config)#arp trusted user-vlan 2-9 translated-vlan 10 FS(config)#arp trusted aging FS(config)#arp trusted 1024
Verification	● Run the **show running-config** command to check whether the configurations take effect.
	FS(config)# show running-config servicetrustedarp arp trusted user-vlan 2-9 translated-vlan 10 arp trusted aging arp trusted 1024

Common Errors

- Trusted ARP is disabled, causing failure to assign ARP entries.

2.4.4 Enabling Gratuitous ARP

Configuration Effect

The interface periodically sends gratuitous ARP packets.

Configuration Steps

- Optional.
- When a switch acts as the gateway, enable gratuitous ARP on an interface to prevent other users from learning incorrect gateway MAC address in case of ARP spoofing.
- Enable gratuitous ARP in interface configuration mode.

Verification

Run the **show running-config interface** *<name>* command to check whether the configuration is successful.

Related Commands

Enabling Gratuitous ARP

Command	**arp gratuitous-send interval** *seconds* [*number*]
Parameter Description	*seconds*: Indicates the interval for sending a gratuitous ARP request. The unit is second. The value ranges from 1 to 3,600. *number*: Indicates the number of gratuitous ARP requests that are sent. The default value is 1. The value ranges from 1 to 100.
Command Mode	Interface configuration mode
Usage Guide	If a network interface of a device acts as the gateway for downstream devices but a downstream device pretends to be the gateway, enable gratuitous ARP on the interface to advertise itself as the real gateway.

Configuration Example

Scenario	For the network topology, see Figure 2- 1.
Configuration Steps	Configure the GigabitEthernet 0/0 interface to send a gratuitous ARP packet every 5 seconds.
	FS(config-if-GigabitEthernet 0/0)#arp gratuitous-send interval 5
Verification	Run the **show running-config interface** command to check whether the configuration takes effect.
	FS#sh running-config interface gigabitEthernet 0/0 Building configuration... Current configuration : 127 bytes ! interface GigabitEthernet 0/0 duplex auto speed auto ip address 30.1.1.1 255.255.255.0 arp gratuitous-send interval 5

2.4.5 Enabling Proxy ARP

Configuration Effect

The device acts as a proxy to reply to ARP request packets from other users.

Notes

By default, Proxy ARP is disabled on Layer-3 switches while enabled on routers.

Configuration Steps

- Optional.
- If a user without any route information needs to obtain the MAC addresses of the IP users in other subnets, enable Proxy ARP on the device so that the device can act as a proxy to send ARP replies.
- Enable Proxy ARP in interface configuration mode.

Verification

Run the **show ip interface** *<name>* command to check whether the configuration takes effect.

Related Commands

↘ **Enabling Proxy ARP**

Command	**ip proxy-arp**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Scenario	For the network topology, see Figure 2- 1.
Configuration Steps	Enable Proxy ARP on port GigabitEthernet 0/0 .
	FS(config-if-GigabitEthernet 0/0)#ip proxy-arp
Verification	Run the **show ip interface** command to check whether the configuration takes effect.

```
FS#show ip interface gigabitEthernet 0/0
GigabitEthernet 0/0
  IP interface state is: DOWN
  IP interface type is: BROADCAST
  IP interface MTU is: 1500
  IP address is:
    No address configured
  IP address negotiate is: OFF
  Forward direct-broadcast is: OFF
  ICMP mask reply is: ON
  Send ICMP redirect is: ON
  Send ICMP unreachable is: ON
  DHCP relay is: OFF
  Fast switch is: ON
  Help address is: 0.0.0.0
  Proxy ARP is: ON
ARP packet input number: 0
  Request packet        : 0
  Reply packet          : 0
  Unknown packet        : 0
TTL invalid packet number: 0
ICMP packet input number: 0
 Echo request          : 0
 Echo reply            : 0
 Unreachable           : 0
 Source quench         : 0
 Routing redirect      : 0
```

2.4.6 Enabling Any IP ARP

Configuration Effect

Users can access the network with any IP address.

Notes

Any IP ARP is supported only on egress gateway products.

In the following two scenarios, users must modify the configuration before they can access the network.

1. The user's IP address is in the same network segment as the interface directly connected to the device. However, the IP address configured on the interface directly connected to the device is not the gateway address.
2. The user's IP address is not in the same network segment as the interface directly connected to the device, but in the network segment of another interface. That means an IP address conflict occurs.

As the user' IP address is not in the same network segment as the interface directly connected to the device, the dynamic ARP entries and direct routes are generated only when the user initiates ARP requests. Therefore, in some scenarios (including but not limited to the following ones), the user will not be able to access the network unless it clears the ARP entries and relearn the gateway address.

1. The device acts as a proxy to respond to ARP requests. After the user learns the MAC address of the device, dynamic ARP entries are cleared on the device. As a result, the user's dynamic ARP entries and direct routes are removed and the user cannot receive the reply packets.
2. The device acts as a proxy to respond to ARP requests. After the user learns the MAC address of the device, any IP ARP is disabled and then enabled again on the interface.

Note: Disabling any IP ARP on an interface will cause users' dynamic ARP entries and direct routes to be removed. Consequently, users cannot receive response packets.

On the other hand, if static ARP entries or ARP entries with VRRP IP addresses exist, dynamic ARP entries generated by any IP ARP will be overwritten or fail to be added, disabling the any IP ARP function.

Configuration Steps

- Optional.
- In a hotel, enable any IP ARP on the gateway so that users can access the network without changing the IP address.
- Enable any IP ARP in interface configuration mode.

Verification

Run the **show running-config interface** *<name>* command to check whether the configuration takes effect.

Related Commands

Enabling Any IP ARP

Command	**arp any-ip**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Disabling any IP ARP on an interface will cause users' dynamic ARP entries and direct routes to be removed. Consequently, users cannot receive response packets. If static ARP entries or ARP entries with VRRP IP addresses exist, dynamic ARP entries generated by any IP ARP will be overwritten or fail to be added, disabling the any IP ARP function.

Configuration Example

Scenario	For the network topology, see Figure 2- 1.

Configuration Steps	Enable any IP ARP on port GigabitEthernet 0/0.
	FS(config-if-GigabitEthernet 0/0)#arp any-ip
Verification	Run the **show running-config interface** command to check whether the configuration takes effect.
	FS(config-if-GigabitEthernet 0/0)#sh run int gi0/0 Building configuration... Current configuration : 140 bytes ! interface GigabitEthernet 0/0 duplex auto speed auto ip address 30.1.1.1 255.255.255.0 arp gratuitous-send interval 5 arp any-ip

2.4.7 Enabling ARP Trustworthiness Detection

Configuration Effect

Enable ARP trustworthiness detection. If the device receiving an ARP request packet fails to find the corresponding entry, it performs NUD. If the MAC address in the existing dynamic ARP entry is updated, the device immediately performs NUD to prevent ARP attacks.

Notes

Since this function adds a strict confirmation procedure in the ARP learning process, it affects the efficiency of ARP learning.

Configuration Steps

- Optional.
- If there is a need for learning ARP entries, enable ARP trustworthiness detection on the device. If the device receiving an ARP request packet fails to find the corresponding entry, it needs to send a unicast ARP request packet to check whether the peer end exists. If yes, the device learns the ARP entry. If not, the device does not learn the ARP entry. If the MAC address in the ARP entry changes, the device will immediately perform NUD to prevent ARP spoofing.
- Enable ARP trustworthiness detection in interface configuration mode.

Verification

Run the **show running-config interface** *<name>* command to check whether the configuration take effect

Related Commands

Enabling ARP Trustworthiness Detection

Command	**arp trust-monitor enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Enable this function. If the corresponding ARP entry exists and the MAC address is not updated, the device does not perform NUD. Enable this function. If the MAC address of the existing dynamic ARP entry is updated, the device immediately performs NUD. After this function is disabled, the device does not perform NUD for learning or updating ARP entries.

Configuration Example

Scenario	For the network topology, see Figure 2- 1.
Configuration Steps	Enable ARP trustworthiness detection on port GigabitEthernet 0/0.
	FS(config-if-GigabitEthernet 0/0)#arp trust-monitor enable
Verification	Run the **show running-config interface** command to check whether the configuration takes effect.
	FS#show running-config interface gigabitEthernet 0/0 Building configuration... Current configuration : 184 bytes ! interface GigabitEthernet 0/0 duplex auto speed auto ip address 30.1.1.1 255.255.255.0 arp trust-monitor enable

2.4.8 Disabling Dynamic ARP Learning

Configuration Effect

After dynamic ARP learning is disabled on an interface, the interface does not learn dynamic ARP entries.

Configuration Steps

- Optional.
- Enable dynamic ARP learning in interface configuration mode.

Verification

Run the **show running-config interface** *<name>* command to check whether the configuration takes effect.

Related Commands

Disabling Dynamic ARP Learning

Command	**noarp-learning enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	If the device has learned the dynamic ARP entries and converted the ARP entries into static ARP entries through Web, disable dynamic ARP learning. Otherwise, enable dynamic ARP learning. After this function is enabled, users can convert dynamic ARP entries into static ARP entries through Web. Users can also use the **clear arp** command to clear ARP entries to deny a user Internet access. If the **clear arp** command is not configured, dynamic ARP entries will be cleared when the timeout expires. After the dynamic ARP learning function is disabled on an interface, the any IP ARP and ARP trustworthiness detection functions will not work.

Configuration Example

Scenario	For the network topology, see Figure 2- 1.
Configuration Steps	Disable dynamic ARP entry learning on port GigabitEthernet 0/0.
	FS(config-if-GigabitEthernet 0/0)#no arp-learning enable
Verification	Run the **show running-config interface** command to check whether the configuration takes effect.
	FS#sh running-config interface gigabitEthernet 0/0 Building configuration... Current configuration : 127 bytes ! interface GigabitEthernet 0/0 duplex auto speed auto ip address 30.1.1.1 255.255.255.0 no arp-learning enable

2.4.9 Enabling ARP Scanning

Configuration Effect

After ARP scanning is enabled on an interface, the device scans neighbors in the specified range and learns the ARP entries of these neighbors.

Configuration Steps

- Optional.
- Enable ARP scanning in interface configuration mode.

Verification

Run the **show running-config interface** *<name>* command to check whether the configuration takes effect.

Related Commands

Enabling ARP Scanning

Command	**arp scan** [*start-ip-address end-ip-address*]
Parameter Description	*start-ip-address*: Indicates the start IP address of ARP scanning range. The start IP address must be smaller than or equal to the end IP address. *end-ip-address*: Indicates the end IP address of ARP scanning range. The end IP address must be greater than or equal to the start IP address.
Command Mode	Interface configuration mode
Usage Guide	1. This function is usually used together with the web-based dynamic-to-static ARP conversion function. 2. The neighbors whose ARP entries are learned are not scanned. 3. If users know the IP address range assigned to their neighbors in the LAN, they can specify the ARP scanning range to scan their neighbors, thereby reducing the waiting time. The number of users in the ARP scanning range must not exceed 1,024. 4. The start and end IP addresses must be in the same network segment as the IP address of the interface (primary or secondary IP address). 5. If the start and end IP addresses are not specified, only the neighbors in the network segment of the primary IP address are scanned. The subnet mask of the primary IP address must consist of at least 22 bits. 6. One ARP scanning configuration takes effect only once. It cannot be saved and loses effect the next time. 7. ARP scanning takes effect when the Layer-3 interface is UP (that is, the link is UP and configured with an IP address).

Configuration Example

Scenario	For the network topology, see Figure 2- 1.
Configuration Steps	Enable ARP scanning on port GigabitEthernet 0/0.
	FS(config-if-GigabitEthernet 0/0)#arp scan 192.168.23.1 192.168.23.10
Verification	Run the **show running-config interface** command to check whether the configuration takes effect.
	FS#sh running-config interface gigabitEthernet 0/0 Building configuration... Current configuration : 127 bytes !

	interface GigabitEthernet 0/0 duplex auto speed auto ip address 192.168.23.2 255.255.255.0 arp scan 192.168.23.1 192.168.23.10

Common Errors

1. The start IP address must be greater than the end IP address in the configured ARP scanning range.

2. The start and end IP addresses are in a different network segment from the IP address of the interface.

2.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears dynamic ARP entries. In gateway authentication mode, dynamic ARP entries in authentication VLANs are not cleared.	**clear arp-cache**

Displaying

Description	Command
Displays the ARP table in detail.	**show arp** [**detail**] [*interface-type interface-number* [*ip* [*mask*] | *mac-address* | **static** | **complete** | **incomplete**]
Displays the ARP table.	**show ip arp**
Displays the trusted ARP table.	**show arp** [**detail**] **trusted** [*ip* [*mask*]]
Displays the ARP entry counter.	**show arp counter**
Displays the timeout of dynamic ARP entries.	**show arp timeout**

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs ARP packet sending and receiving.	**debug arp**
Debugs the creation and deletion of ARP entries.	**debug arp event**

3 Configuring IP Event Dampening

3.1 Overview

When the Layer-3 port on a Layer-3 device frequently goes Up and Down due to manual enabling/disabling or other external causes, the routing table on the device will flap repeatedly. If a routing protocol is configured, the protocol may propagate the flap to the entire network, causing repeated updates and recalculation of neighboring routes, which wastes network bandwidths and destabilizes the network. Repeated route updates and recalculation on devices consume many CPU resources, which affects the normal running of customer networks.

IP Event Dampening detects abnormal Up/Down flapping and automatically suppresses frequent port state changes, which prevents the propagation of single-point link failures by a routing protocol. When the port is restored, it will be automatically unsuppressed, thus reducing network flaps and CPU resource consumption while improving network stability.

Protocols and Standards

N/A

3.2 Applications

Application	Description
Routed Port Flap Dampening	Monitors the state change of the Layer-3 port on a router, and suppresses frequent port flapping.

3.2.1 Routed Port Flap Dampening

Scenario

In a network that runs a routing protocol, when a port on a router connected to another router frequently goes Up and Down, neighboring routes will be repeatedly updated and recalculated. The routing protocol may propagate the flap to the entire network, causing a network flap. IP Event Dampening can be enabled on the connected routers to monitor port state changes and suppress frequent port flapping, thus reducing network flaps and CPU resource consumption while improving network stability.

Figure 3- 1

Remarks	A and B are routers.

Deployment

Configure IP Event Dampening on portGE0/1 on Router A and portGE0/1 on Router B respectively.

The subinterfaces and the virtual templates of interfaces on routers do not support the dampening feature.

3.3 Features

Basic Concepts

Penalty

A port that goes Up or Down gets a penalty for each state change, but the penalty decays exponentially when the port is stable. In this way, port behaviors can be sensed and controlled intelligently.

Suppress Threshold

When the cumulative penalty of a port exceeds a suppress threshold, the port is considered to flap and will be suppressed.

Half-Life Period

The half-life period is the period required for the penalty to decrease to half of the original value when the port is stable. It defines the speed at which the penalty decays exponentially. The shorter the half-life period, the faster the penalty decays, and the faster the port is detected to be stable, but the flap detection sensitivity is reduced.

Reuse Threshold

When the port no long flaps and its penalty decays to a certain degree (below the suppress threshold), the port is considered to be stable and is unsuppressed.

Maximum Suppress Time

When a port keeps flapping and reaches a very large penalty, the port will not be usable for a long time. To avoid this problem, the maximum suppress time is defined to always maintain the port suppression duration below a certain value no matter how long the port has flapped.

Overview

Feature	Description
Port Flap Suppression	Configure the criteria and parameters of flap suppression on ports to enable switches or routers to identify and suppress frequently flapping ports, which ensures route stability and avoids route flap propagation.

3.3.1 Port Flap Suppression

Working Principle

A port configured with IP Event Dampening is assigned a penalty. The port gets a penalty of 1,000 each time when it goes Down, but the penalty decreases with time. If the port goes Down again, the penalty increases accordingly. When the cumulative penalty exceeds the suppress threshold, the port will be suppressed. For the affected upper-layer protocol, the suppressed port is always Down no matter what the actual port state is. When the penalty decreases to the reuse threshold, the port will be unsuppressed, and the upper-layer protocol can sense the actual port state.

If a Layer-3 port is not configured with IP Event Dampening, or is not suppressed by it, the routing protocol or other protocol concerned about the port status still work normally. When the port is suppressed, the upper-layer protocol considers the port to be Down. Any state change of the port before the port is unsuppressed does not affect the routing table and the route calculation and advertisement performed by the upper-layer routing protocol.

Related Configuration

Configuring IP Event Dampening

- By default, IP Event Dampening is disabled on Layer-3 ports.
- Run the **dampening** [*half-life-period* [*reuse-threshold suppress-threshold max-suppress* [**restart** [*restart-penalty*]]]] command to enable or disable IP Event Dampening on Layer-3 ports.

3.4 Configuration

Configuration	Description and Command	
Enabling IP Event Dampening	(Mandatory)It is used to suppress Layer-3 port flapping.	
	dampening	Configures IP Event Dampening.

3.4.1 Enabling IP Event Dampening

Configuration Effect

When a port configured with IP Event Dampening keeps flapping until the predefined threshold is exceeded, the port is set to Down.

Notes

- When a Layer-3 port on a switch is converted to a Layer-2 port (for example, from a routed port to a switch port), the IP Event Dampening configuration on the port will be deleted.
- Only the main interface on a router can be configured with IP Event Dampening. The configuration takes effect for all subinterfaces of the main interface, but you cannot run the **dampening** command directly on subinterfaces and virtual templates.

Configuration Steps

Configuring IP Event Dampening

- Mandatory.
- Perform the configuration in Layer-3 interface configuration mode.
- You can specify the half-life period, reuse threshold, suppress threshold, maximum suppress time, and initial penalty. If you do not set these parameters, their default values will be used.

Verification

Use any one of the following commands to check whether the configuration takes effect:

- **show running-config**
- **show interfaces** [*interface-id*] **dampening**, which is used to check the IP Event Dampening configuration on a specified port

Related Commands

Enabling IP Event Dampening on a Port

Command	**dampening** [*half-life-period* [*reuse-threshold suppress-threshold max-suppress* [**restart** [*restart-penalty*]]]]
Parameter Description	*half-life-period*: Indicates the half-life period. Value range: <1–30>; default value: 5s. *reuse-threshold:* Indicates the reuse threshold. Value range: <1–20,000>; default value: 1,000.

	suppress-threshold: Indicates the suppress threshold. Value range: <1–20,000>; default value: 2,000. *max-suppress:* Indicates the maximum suppress time. Value range: <1–255>; default value: four times the half-life period. **restart** *restart-penalty:* Indicates the initial penalty. Value range: <1–20,000>; default value: 2,000.
Command Mode	Interface configuration mode
Usage Guide	IP Event Dampening can affect direct routes, host routes, static routes, dynamic routes, and VRRP. When a port is suppressed based on the configured criteria, the affected modules determine that the port is Down and therefore delete corresponding routes. No data packet will be transmitted through the port. When the **dampening** command is rerun on a port configured with IP Event Dampening, the dampening information on the port will be cleared, but the flap count is retained, unless you use the **clear counters** command to clear the counters on the port. If the **max-suppress** parameter is set to a very small value, making the maximum penalty smaller than the suppress threshold, the port will never be suppressed. When such a configuration error occurs, the following message indicating a configuration failure will be printed: % Maximum penalty (10) is less than suppress penalty (2000). Increase maximum suppress time If the available system memory is insufficient to run the **dampening** command, the following message indicating a configuration failure will be printed: % No memory, configure dampening fail!

Configuration Example

Configuring IP Event Dampening on Layer-3 Ports

Scenario **Figure 3- 2**	
Configuration Steps	Enable IP Event Dampening on port GigabitEthernet 0/1 on Router A and on port GigabitEthernet 0/1 on Router B respectively, and set **half-time-period** to 30s, **reuse-threshold** to 1,500, **suppress-threshold** to 10,000, and **max-suppress** to 120s.
A	FS(config)#interface GigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)#dampening 30 1500 10000 100
B	FS(config)#interface GigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)#dampening 30 1500 10000 100
Verification	Run the **show interfaces dampening** command to check the IP Event Dampening configuration on the corresponding ports.
	FS#show interfaces dampening

	GigabitEthernet 0/1 Flaps Penalty Supp ReuseTm HalfL ReuseV SuppV MaxSTm MaxP Restart 0 0 FALSE 0 30 1500 1000 100 15119 0

Common Errors

- The port on a Layer-3 switch is not converted to a routed port by using the **no swithport** command before IP Event Dampening is configured.

3.5 Monitoring

Clearing

Description	Command
Clears the interface counters.	**clear counters**

For details about the **clear counter** command, see the related chapter for the "Interface" command.

Displaying

Description	Command
Displays the counters on suppressed ports.	**show dampening interface**
Displays the IP Event Dampening configuration on ports.	**show interfaces dampening**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Enables debugging of IP Event Dampening.	**debug dampening interface**

4 Configuring TCP

4.1 Overview

The Transmission Control Protocol (TCP) is a transport-layer protocol providing reliable connection-oriented and IP-based services to for the application layer.

Internetwork data flows in 8-bit bytes are sent from the application layer to the TCP layer, and then fragmented into packet segments of a proper length via the TCP. The Maximum Segment Size (MSS) is usually limited by the Maximum Transmission Unit (MTU) of the data link layer. After that, the packets are sent to the IP layer and then to the TCP layer of a receiver through the network.

To prevent packet loss, every byte is identified by a sequence number via the TCP, and this ensures that packets destined for the peer are received in order. Then, the receiver responds with a TCP ACK packet upon receiving a packet. If the sender does not receive ACK packets in a reasonable Round-Trip Time (RTT), the corresponding packets (assumed lost) will be retransmitted.

- TCP uses the checksum function to check data integrity. Besides, MD5-based authentication can be used to verify data.
- Timeout retransmission and piggyback mechanism are adopted to ensure reliability.
- The Sliding Window Protocol is adopted to control flows. As documented in the Protocol, unidentified groups in a window should be retransmitted.

Protocols and Standards

- RFC 793: Transmission Control Protocol
- RFC 1122: Requirements for Internet Hosts -- Communication Layers
- RFC 1191: Path MTU Discovery
- RFC 1213: Management Information Base for Network Management of TCP/IP-based Internets: MIB-II
- RFC 4022: Management Information Base for the Transmission Control Protocol (TCP)

4.2 Applications

Application	Description
Optimizing TCP Performance	To avoid TCP packet fragmentation on a link with a small MTU, Path MTU Discovery (PMTUD) is enabled.
Detecting TCP Connection Exception	TCP checks whether the peer works normally.

4.2.1 Optimizing TCP Performance

Scenario

For example, TCP connection is established between A and D, as shown in the following figure. The MTU of the link between A and B is 1500 bytes, 1300 bytes between B and C, and 1500 bytes between C and D. To optimize TCP transmission performance, packet fragmentation should be avoided between B and C.

Figure 4- 1

Remarks:	A, B, C and D are routers.

Deployment

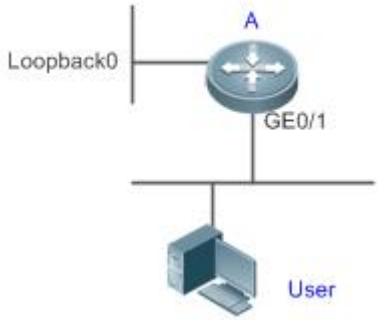
- Enable PMTUD on A and D.

4.2.2 Detecting TCP Connection Exception

Scenario

For example, in the following figure, User logs in to A through telnet but is shut down abnormally, as shown in the following figure. In case of TCP retransmission timeout, the User's TCP connection remains for a long period. Therefore, TCP keepalive can be used to rapidly detect TCP connection exception.

Figure 4- 2



Remarks:	A is a router.

Deployment

- Enable TCP keepalive on A.

4.3 Features

Basic Concepts

TCP Header Format

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Source Port          |       Destination Port        |
```

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Sequence Number                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Acknowledgment Number                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Data |           |U|A|P|R|S|F|                               |
| Offset| Reserved  |R|C|S|S|Y|I|            Window             |
|       |           |G|K|H|T|N|N|                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Checksum            |         Urgent Pointer        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             data                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- **Source Port** is a 16-bit source port number.
- **Destination Port** is a 16-bit destination port number.
- **Sequence Number** is a 32-bit sequence number.
- **Acknowledgment Number** is a 32-bit number that identifies the next sequence number that the receiver is expecting to receive.
- **Data Offset** is a 4-bit number that indicates the total number of bytes in the TCP header (option included) divided by 4.
- A flag bit is 6-bit. URG: the urgent pointer field is significant; ACK: the acknowledgment field is significant; PSH: indicates the push function; RST: resets TCP connection; SYN: synchronizes the sequence number (establishing a TCP connection); FIN: no more data from the sender (closing a TCP connection).
- A 16-bit Window value is used to control flows. It specifies the amount of data that may be transmitted from the peer between ACK packets.
- **Checksum** is a 16-bit checksum.
- **Urgent Pointer** is 16-bit and shows the end of the urgent data so that interrupted data flows can continue. When the URG bit is set, the data is given priority over other data flows.

TCP Three-Way Handshake

- The process of TCP three-way handshake is as follows:

3. A client sends a SYN packet to the server.
4. The server receives the SYN packet and responds with a SYN ACK packet.
5. The client receives the SYN packet from the server and responds with an ACK packet.

- After the three-way handshake, the client and server are connected successfully and ready for data transmission.

Overview

Feature	Description
Configuring SYN Timeout	Configure a timeout waiting for a response packet after an SYN or SYN ACK packet is sent.
Configuring Window Size	Configure a window size.
Configuring Reset Packet Sending	Configure the sending of TCP reset packets after receiving port unreachable messages.
Configuring MSS	Configure an MSS for TCP connection.
Configuring MSS Value for SYN Packet	Modify the MSS value in a SYN packet.
Path MTU Discovery	Discover the smallest MTU on TCP transmission path, and adjust the size of TCP packets based on this MTU to avoid fragmentation.
TCP Keepalive	Check whether the peer works normally.

4.3.1 Configuring SYN Timeout

Working Principle

A TCP connection is established after three-way handshake: The sender sends an SYN packet, the receiver replies with a SYN ACK packet, and then the sender replies with an ACK packet.

- If the receiver does not reply with a SYN ACK packet after the sender sends an SYN packet, the sender keeps retransmitting the SYN packet for certain times or until timeout period expires.
- If the receiver replies with a SYN ACK packet after the sender sends an SYN packet but the sender does not reply with an ACK packet, the receiver keeps retransmitting the SYN ACK packet for certain times or until timeout period expires. (This occurs in the case of SYN flooding.)

Related Configuration

Configuring TCP SYN Timeout

- The default TCP SYN timeout is 20 seconds.
- Run the **ip tcp synwait-time** *seconds* command in global configuration mode to configure an SYN timeout ranging from 5 to 300 seconds.
- In case of SYN flooding, shortening SYN timeout reduces resource consumption. However, it does not work in continuous SYN flooding. When a device actively makes a request for a connection with an external device, through telnet for example, shortening SYN timeout reduces user's wait time. You may prolong SYN timeout properly on a poor network.

The **ip tcp syntime-out** command in version 10.x is disused but compatible in version 11.0. If this command is executed, it will be converted to the **ip tcp synwait-time** command.

4.3.2 Configuring Window Size

Working Principle

Data from the peer is cached in the TCP receiving buffer and subsequently read by applications. The TCP window size indicates the size of free space of the receiving buffer. For wide-bandwidth bulk-data connection, enlarging the window size dramatically promotes TCP transmission performance.

Related Configuration

Configuring Window Size

- Run the **ip tcp window-size** *size* command in global configuration mode to configure a window size ranging from 128 to (65535<< 14) bytes. The default is 65535 bytes. If the window size is greater than 65535 bytes, window enlarging will be enabled automatically.
- The window size advertised to the peer is the smaller value between the configured window size and the free space of the receiving buffer.

4.3.3 Configuring Reset Packet Sending

Working Principle

When TCP packets are distributed to applications, if the TCP connection a packet belongs to cannot be identified, the local end sends a reset packet to the peer to terminate the TCP connection. Attackers may use port unreachable messages to attack the device.

Related Configuration

Configuring the Sending of TCP Reset Packets After Receiving Port Unreachable Messages

By default, TCP reset packet sending upon receiving port unreachable messages is enabled.

Run the **no ip tcp send-reset** command in global configuration mode to disable TCP reset packet sending upon receiving port unreachable messages.

After this function is enabled, attackers may use port unreachable messages to attack the device.

The **ip tcp not-send-rst** command in version 10.x is disused but compatible in version 11.0. If this command is executed, it will be converted to the **no ip tcp send-reset** command.

4.3.4 Configuring MSS

Working Principle

The MSS refers to the total amount of data contained in a TCP segment t excluding TCP options.

Three-way handshake is implemented through MSS negotiation. Both parties add the MSS option to SYN packets, indicating the largest amount of data that the local end can handle, namely, the amount of data allowed from the peer. Both parties take the smaller MSS between them as the advertised MSS.

The MSS value is calculated as follows:

- IPv4 TCP: MSS = Outgoing interface MTU –IP header size (20-byte)–TCP header size (20-byte).

The effective MSS is the smaller one between the calculated MSS and the configured MSS.

If a connection supports certain options, the option length (with **data offset** taken into consideration) should be deducted from an MSS value. For example, 20 bytes for MD5 digest (with **data offset** taken into consideration) should be subtracted from the MSS.

Related Configuration

Configuring MSS

- Run the **ip tcp mss** *max-segment-size* command in global configuration mode to set an MSS. It ranges from 68 to 1000 bytes. By default, the MSS is calculated based on MTU. If an MSS is configured, the effective MSS is the smaller one between the calculated MSS and the configured MSS.
- An excessively small MSS reduces transmission performance. You can promote TCP transmission by increasing the MSS. Choose an MSS value by referring to the interface MTU. If the former is bigger, TCP packets will be fragmented and transmission performance will be reduced.

4.3.5 Configuring MSS Value for SYN Packet

Working Principle

When a client initiates a TCP connection, it negotiates with the server on the total amount of data contained in a TCP segment through the MSS field in TCP SYN packets. The MSS value in the SYN packets indicates the largest amount of data that the server sends in a single and unfragmented piece.

For example, in the following figure, the MSS negotiated between a PC and a HTTP server is 1460, but TCP packets carrying 1460-byte data should be fragmented as they cannot directly pass R1 and R2 connected by a tunnel with an MTU of less than 1500. Modify the MSS value in SYN packets on interfaces (1) and (2) of R2 to enable TCP packets to pass R1 and R2.

Figure 4- 3

Related Configuration

Configuring MSS Value for TCPv4 SYN Packets

- By default, the MSS value in TCPv4 SYN packets is not modified.
- Run the **ip tcp adjust-mss** *max-segment-size* command in interface configuration mode to set an MSS, which ranges from 500 to 1460 bytes.
- To avoid packet fragmentation in the case of a small path MTU, you may configure an MSS for TCPv4 SYN packets. The MSS in TCPv4 SYN packets will change to the configured value once the device receives the packets. You may configure an MSS value with reference to the interface MTU.

This configuration applies to a new connection but does not take effect for an existing TCP connection.

4.3.6 Path MTU Discovery

Working Principle

The Path MTU Discovery f stipulated in RFC1191 is used to discover the smallest MTU in a TCP path to avoid fragmentation, enhancing network bandwidth utilization. The process of TCPv4 Path MTU Discovery is described as follows:

1. The source sends TCP packets with the Don't Fragment (DF) bit set in the outer IP header.

2. If the outgoing interface MTU value of a router in the TCP path is smaller than the IP packet length, the packet will be discarded and an ICMP error packet carrying this MTU will be sent to the source.
3. Through parsing the ICMP error packet, the source knows the smallest MTU in the path (path MTU) is.
4. The size of subsequent data segments sent by the source will not surpass the MSS, which is calculated as follows: TCP MSS = Path MTU – IP header size – TCP header size.

Related Configuration

Enabling Path MTU Discovery

By default, Path MTU Discovery is disabled.

Run the **ip tcp path-mtu-discovery** command to enable PMTUD in global configuration mode.

4.3.7 TCP Keepalive

Working Principle

You may enable TCP keepalive to check whether the peer works normally. If a TCP end does not send packets to the other end for a period of time (namely idle period), the latter starts sending keepalive packets successively to the former for several times. If no response packet is received, the TCP connection is considered inactive and then closed.

Related Configuration

Enabling Keepalive

- By default, TCP keepalive is disabled.
- Run the **ip tcp keepalive** [**interval** *num1*] [**times** *num2*] [**idle-period** *num3*] command to in global configuration mode to enable TCP keepalive. See **Configuration** for parameter description.

The **service tcp-keepalives-in** command is used in version 10.x to enable keeplive on the TCP server. It is disused but compatible in version 11.0. If this command is executed, it will be converted to the **ip tcp keepalive** [**interval** *num1*] [**times** *num2*] [**idle-period** *num3*] command.

The **service tcp-keepalives-out** command is used in version 10.x to enable keeplive on the TCP client. It is disused but compatible in version 11.0. If this command is executed, it will be converted to the **ip tcp keepalive** [**interval** *num1*] [**times** *num2*] [**idle-period** *num3*] command.

This command applies to both TCP server and client.

4.4 Configuration

Configuration	Description and Command	
Optimizing TCP Performance	(Optional) It is used to optimize TCP connection performance.	
	ip tcp synwait-time	Configures a timeout for TCP connection.
	ip tcp window-size	Configures a TCP window size.
	ip tcp send-reset	Configures the sending of TCP reset packets after receiving port unreachable messages.

	ip tcp mss	Configures an MSS for TCP connection.
	ip tcp adjust-mss	Configures an MSS value for the TCPv4 SYN packets
	ip tcp path-mtu-discovery	Enables Path MTU Discovery.
Detecting TCP Connection Exception	(Optional) It is used to detect whether the peer works normally.	
	ip tcp keepalive	Enables TCP keepalive.

4.4.1 Optimizing TCP Performance

Configuration Effect

- Ensure optimal TCP performance and prevent fragmentation.

Notes

N/A

Configuration Steps

Configuring SYN Timeout

- Optional.
- Configure this on the both ends of TCP connection.

Configuring TCP Window Size

- Optional.
- Configure this on the both ends of TCP connection.

Configuring the Sending of TCP Reset Packets After Receiving Port Unreachable Messages.

- Optional.
- Configure this on the both ends of TCP connection.

Configuring MSS

- Optional.
- Configure this on the both ends of TCP connection.

Configuring MSS Value for TCPv4 SYN Packets

- Optional.
- If the MTU between two routers in TCP transmission is small, you may configure an MSS value on the routers.

Enabling Path MTU Discovery

- Optional.
- Configure this on the both ends of TCP connection.

Verification

N/A

Related Commands

Configuring SYN Timeout

Command	**ip tcp synwait-time** *seconds*
Parameter Description	*seconds*: Indicates SYN packet timeout. It ranges from 5 to 300 seconds. The default is 20 seconds.
Command Mode	Global configuration mode
Usage Guide	In case of SYN flooding, shortening SYN timeout reduces resource consumption. However, it does not work in continuous SYN flooding. When a device actively makes a request for a connection with an external device, through telnet for example, shortening SYN timeout reduces user's wait time. You may prolong SYN timeout properly on a poor network.

Configuring TCP Window Size

Command	**ip tcp window-size** *size*
Parameter Description	*size*: Indicates a TCP window size. It ranges from 128 to (65535 << 14) bytes. The default is 65535 bytes.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Sending of TCP Reset Packets After Receiving Port Unreachable Messages

Command	**ip tcp send-reset**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, TCP reset packet sending upon receiving port unreachable messages is enabled.

Configuring MSS

Command	**ip tcp mss** *max-segment-size*
Parameter Description	*max-segment-size*: Indicates the maximum segment size. It ranges from 68 to 10000 bytes. By default, the MSS is calculated based on MTU.
Command Mode	Global configuration mode
Usage Guide	This command defines the MSS for a TCP communication to be established. The negotiated MSS for a new connection should be smaller than this MSS. If you want to reduce the MSS, run this command. Otherwise, do not perform the configuration.

Configuring MSS Value for TCPv4 SYN Packets

Command	**ip tcp adjust-mss** *max-segment-size*
Parameter Description	*max-segment-size*: Indicates the maximum segment size, ranging from 500 to 1460 bytes
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring Path MTU Discovery

Command	**ip tcp path-mtu-discovery** [**age-timer** *minutes* | **age-timer infinite**]
Parameter Description	**age-timer** *minutes*: Indicates the interval for a new probe after a path MTU is discovered. It ranges from 10 to 30 minutes. The default is 10 minutes. **age-timer infinite**: No probe is implemented after a path MTU is discovered.
Command Mode	Global configuration mode
Usage Guide	The PMTUD is an algorithm documented in RFC1191 aimed to improve bandwidth utilization. When the TCP is applied to bulk data transmission, this function may facilitate transmission performance. If the MSS used for the connection is smaller than what the peer connection can handle, a larger MSS is tried every time the age timer expires. The age timer is a time interval for how often TCP estimates the path MTU with a larger MSS. The discovery process is stopped when either the send MSS is as large as the peer negotiated, or the user has disabled the timer on the router. You may turn off the timer by setting it to **infinite**.

Configuration Example

Enabling Path MTU Discovery

Configuration Steps	Enable PMTUD for a TCP connection. Adopt the default age timer settings.
	FS# configure terminal FS(config)# ip tcp path-mtu-discovery FS(config)# end
Verification	Run the **show tcp pmtu** command to display the IPv4 TCP PMTU.
	FS# show tcp pmtu Number Local Address Foreign Address PMTU 1 192.168.195.212.23 192.168.195.112.13560 1440

Common Errors

N/A

4.4.2 Detecting TCP Connection Exception

Configuration Effect

- Check whether the peer works normally.

Notes

N/A

Configuration Steps

Enabling TCP Keepalive

- Optional.

Verification

N/A

Related Commands

Enabling TCP Keepalive

Command	**ip tcp keepalive** [**interval** *num1*] [**times** *num2*] [**idle-period** *num3*]
Parameter Description	**interval** *num1*: Indicates the interval to send keepalive packets. Ranging from 1 to120 seconds. The default is 75 seconds. **times** *num2*: Indicates the maximum times for sending keepalive packets. It ranges from 1 to 10. The default is 6. **idle-period** *num3*: Indicates the time when the peer sends no packets to the local end, It ranges from 60 to 1800 seconds. The default is15 minutes.
Command Mode	Global configuration mode
Usage Guide	You may enable TCP keepalive to check whether the peer works normally. The function is disabled by default. Suppose a user enables TCP keepalive function with the default interval, times and idle period settings. The user does not receive packets from the other end within 15 minutes and then starts sending Keepalive packets every 75 seconds for 6 times. If the user receives no TCP packets, the TCP connection is considered inactive and then closed.

Configuration Example

Enabling TCP Keepalive

Configuration Steps	Enable TCP keepalive on a device with **interval** and **idle-period** set to 3 minutes and 60 seconds respectively. If the user receives no TCP packets from the other end after sending keepalive packets four times, the TCP connection is considered inactive.
	FS# configure terminal FS(config)# ip tcp keepalive interval 60 times 4 idle-period 180 FS(config)# end

Verification	A user logs in to a device through telnet, and then shuts down the local device. Run the **show tcp connect** command on the remote device to observe when IPv4 TCP connection is deleted.

Common Errors

N/A

4.5 Monitoring

Displaying

Description	Command
Displays basic information on IPv4 TCP connection.	**show tcp connect** [**local-ip** *a.b.c.d*] [**local-port** *num*] [**peer-ip** *a.b.c.d*] [**peer-port** *num*]
Displays IPv4 TCP connection statistics.	**show tcp connect statistics**
Displays IPv4 TCP PMTU.	**show tcp pmtu** [**local-ip** *a.b.c.d*] [**local-port** *num*] [**peer-ip** *a.b.c.d*] [**peer-port** *num*]
Displays IPv4 TCP port information.	**show tcp port** [*num*]
Displays IPv4 TCP parameters.	**show tcp parameter**
Displays IPv4 TCP statistics.	**show tcp statistics**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Displays the debugging information on IPv4 TCP packets.	**debug ip tcp packet** [**in** | **out**] [**local-ip** *a.b.c.d*] [**peer-ip** *a.b.c.d*] [**global**][**local-port** *num*] [**peer-port** *num*] [**deeply**]
Displays the debugging information on IPv4 TCP connection.	**debug ip tcp transactions** [**local-ip** *a.b.c.d*] [**peer-ip** *a.b.c.d*] [**local-port** *num*] [**peer-port** *num*]

5 Configuring IPv4/IPv6 REF

5.1 Overview

On products incapable of hardware-based forwarding, IPv4/IPv6 packets are forwarded through the software. To optimize the software-based forwarding performance, FS introduces IPv4/IPv6 express forwarding through software (FS Express Forwarding, namely REF).

REF maintains two tables: forwarding table and adjacency table. The forwarding table is used to store route information. The adjacency table is derived from the ARP table and IPv6 neighbor table, and it contains Layer 2 rewrite(MAC) information for the next hop..

REF is used to actively resolve next hops and implement load balancing.

Protocols and Standards

N/A

5.2 Applications

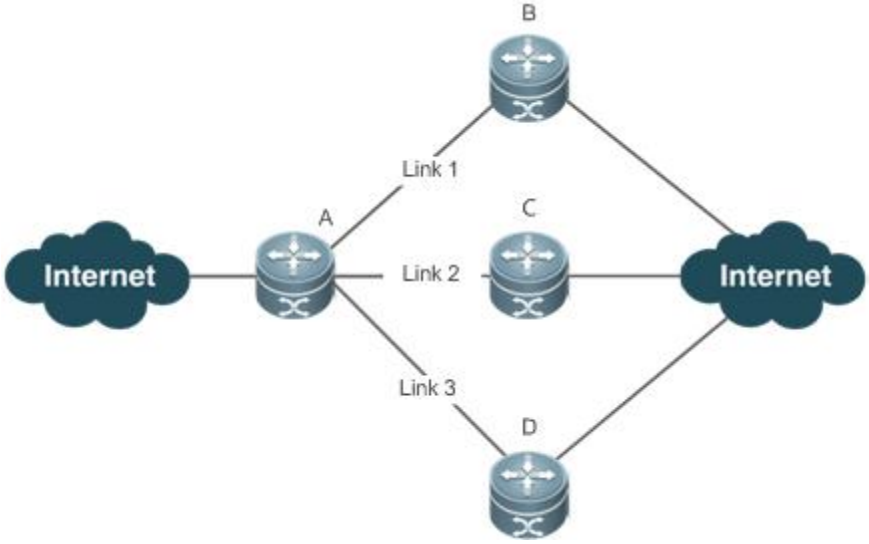
Application	Description
Load Balancing	During network routing, when a route prefix is associated with multiple next hops, REF can implement load balancing among the multiple next hops.

5.2.1 Load Balancing

Scenario

As shown in Figure 5- 1, a route prefix is associated with three next hops on router A, namely, link 1, link 2, and link 3. By default, REF implements load balancing based on the destination IP address. Load balancing can be implemented based on the source IP address and destination IP address as well.

Figure 5- 1



Remarks	A is a router that runs REF. B, C and D are forwarding devices.

Deployment

- Run REF on router A.

5.3 Features

Basic Concepts

IPv4 REF involves the following basic concepts:

Routing table

An IPv4 routing table stores routes to the specific destinations and contains the topology information. During packet forwarding, IPv4 REF selects packet transmission paths based on the routing table.

Adjacent node

An adjacent node contains output interface information about routed packets, for example, the next hop, the next component to be processed, and the link layer encapsulation. When a packet is matched with an adjacent node, the packet is directly encapsulated and then forwarded. For the sake of query and update, an adjacent node table is often organized into a hash table. To support routing load balancing, the next hop information is organized into a load balance entry. An adjacent node may not contain next hop information. It may contain indexes of next components (such as other line cards and multi-service cards) to be processed.

Active resolution

REF supports next hop resolution. If the MAC address of the next hop is unknown, REF will actively resolve the next hop. IPv4 REF requests the ARP module for next hop resolution.

Packet forwarding path

Packets are forwarded based on their IPv4 addresses. If the source and destination IPv4 addresses of a packet are specified, the forwarding path of this packet is determined.

5.3.1 Load Balancing Policies

Load balancing is configured to distribute traffic load among multiple network links.

Working Principle

REF supports two load balancing modes. In the REF model, a route prefix is associated with multiple next hops, in other words, it is a multi-path route. The route will be associated with a load balance table and implement weight-based load balancing. When an IPv4 packet is matched with a load balance entry based on the longest prefix match, REF performs hash calculation based on the IPv4 address of the packet and selects a path to forward the packet.

IPv4 REF supports two kinds of load balancing policies: load balancing based on destination IP address, and load balancing based on the source and destination IP addresses.

Related Configuration

Configuring Load Balancing Based on IPv4 Source and Destination Addresses

- By default, load balancing is implemented based on the IPv4 destination addresses.

- Run the **ip ref load-sharing original** command to configure the load balancing.
- After the configuration, load balancing is implemented based on the IPv4 source and destination addresses.

5.4 Configuration

Configuration	Description and Command	
Configuring Load Balancing Policies	Optional.	
	ip ref load-sharing original	Enables the load balancing algorithm based on IPv4 source and destination addresses.

The preceding commands are router-specific commands.

5.4.1 Configuring Load Balancing Policies

Configuration Effect

REF supports the following two kinds of load balancing policies:

- Destination address-based load balancing indicates performing hash calculation based on the destination address of the packet. The path with a greater weight is more likely to be selected. This policy is used by default.
- Implementing load balancing based on the source and destination addresses indicates performing hash calculation based on the source and destination addresses of the packet. The path with a greater weight is more likely to be selected.

Notes

N/A

Configuration Steps

- Optional.
- Perform this configuration if you want to implement load balancing based on the source and destination IP addresses.
- Perform this configuration on a router that connects multiple links.

Verification

Run the **show ip ref adjacency statistic** command to display the IPv4 load balancing policy.

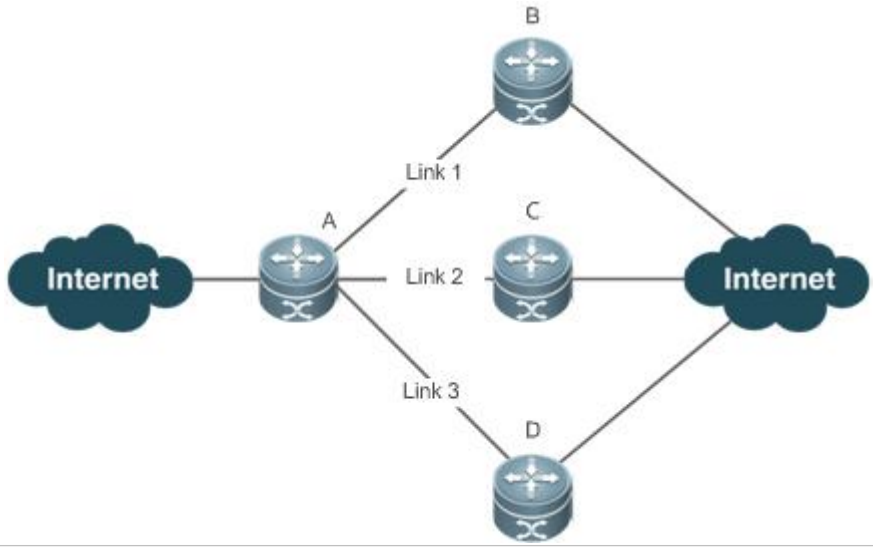
Related Commands

Configuring Load Balancing Based on IPv4 Source and Destination Addresses

Command	ip ref load-sharing original
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring Load Balancing Based on Source and Destination IP Addresses

Scenario Figure 5- 2	
	A route prefix is associated with three next hops on router A, namely, link 1, link 2, and link 3.
Configuration Steps	Configure load balancing based on IPv4 source and destination IP addresses on router A.
A	A#configure terminal Enter configuration commands, one per line. End with CNTL/Z. A(config)#ip ref load-sharing original
Verification	

	A #show ip ref adjacency statistics
	adjacency balance table statistic:
	  source-dest-address load-sharing
	  balance: 0
	
	adjacency node table statistic:
	  total : 3
	  local : 1
	  glean : 0
	  forward: 0
	  discard: 0
	  mcast : 1
	  punt : 1

	bcast : 0

5.5 Monitoring

Displaying REF Packet Statistics

REF packet statistics includes the number of forwarded packets and the number of packets discarded due to various causes. You can determine whether packets are forwarded as expected by displaying and clearing REF packet statistics.

Command	Description
show ip ref packet statistics	Displays IPv4 REF packet statistics.
clear ip ref packet statistics	Clears IPv4 REF packet statistics.

Displaying Adjacency Information

You can run the following commands to display adjacency information:

Command	Description
show ip ref adjacency [**glean** | **local** | *ip-address* | {**interface** *interface_type interface_number*} | **discard** | **statistics**]	Displays the gleaned adjacencies, local adjacencies, adjacencies of a specified IP address, adjacencies associated with a specified interface, and all adjacent nodes in IPv4 REF.

Displaying Active Resolution Information

You can run the following commands to display next hops to be resolved:

Command	Description
show ip ref resolve-list	Displays the next hop to be resolved .

Displaying Packet Forwarding Path Information

Packets are forwarded based on their IPv4/IPv6 addresses. If the source and destination IPv4/IPv6 addresses of a packet are specified, the forwarding path of this packet is determined. Run the following commands and specify the IPv4/IPv6 source and destination addresses of a packet. The forwarding path of the packet is displayed, for example, the packet is discarded, submitted to a CPU, or forwarded. Furthermore, the interface that forwards the packet is displayed.

Command	Description
show ip ref exact-route [**oob**] *source-ipaddress dest_ipaddress*	Displays the forwarding path of a packet. oob indicates out-of-band management network.

Displaying Route Information in an REF Table

Run the following commands to display the route information in an REF table:

Command	Description

show ip ref route [**oob**] [**default** | {*ip mask*}| **statistics**]	Displays route information in the IPv4 REF table. The parameter **default** indicates a default route. oob indicates out-of-band management network.

6 Configuring Tunnel Interfaces

6.1 Overview

Tunnel interfaces are virtual interfaces used to implement tunneling. A tunnel interface provides a standard transmission link and you do not need to specify a transport protocol or payload protocol. Each tunnel interface represents a transmission link.

Tunneling function includes the following parts:

- Payload protocol: Is used to encapsulate the data transmitted in tunnels. For example, the IPv4 and IPv6 protocols work as payload protocols. Generic routing encapsulation (GRE) tunnels can carry IPv4 or IPv6 data.
- Bearer protocol: Is used for secondary encapsulation and identification of the data to be transmitted. Among the tunnels described in this document, only the GRE tunnel uses a bearer protocol, that is, the GRE protocol. The other tunnels use the IPv4 and IPv6 protocols. Packets are encapsulated with outer IPv4 and IPv6 headers.
- Transport protocol: Is used to transmit the data encapsulated for the second time through a bearer protocol. FS products use the widely applied IPv4 and IPv6 protocols as transport protocols.

The tunnel mode can be used to set up communication between two private networks running the same protocol through a heterogeneous public network.

Tunneling is applicable to the following scenarios:

- Because tunneling supports different payload protocols, it allows the communication between local networks running non-IP protocols through a single network (IP network). Because tunneling operates on routes running transport protocols (IP protocols), it allows wider application of the protocols with hop limit.
- Tunneling allows discrete subnets to be connected through a single network (IP network).
- Tunneling allows the virtual private network (VPN) feature to be enabled on wide area networks (WANs).

Encapsulated data is transmitted through tunnels, which is a complex process. In some cases, you need to pay attention to the following changes:

- Because a tunnel is a logical link, it appears to be a single hop in routing. However, actually its path cost may be more than one hop. When you use a tunnel for transmission, note that the route of the tunnel link is different from the actual route.
- When you configure a firewall or an access control list (ACL), take the tunnel configuration into consideration. The transmission bandwidth and maximum transmission unit (MTU) allowed by payload protocols are smaller than the theoretical values.

Protocols and Standards

- RFC2784: Generic Routing Encapsulation (GRE)
- RFC2890: Key and Sequence Number Extensions to GRE
- RFC3056: Connection of IPv6 Domains via IPv4 Clouds
- RFC4023: Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)
- RFC4087: IP Tunnel MIB
- RFC4213: Basic Transition Mechanisms for IPv6 Hosts and Routers

- RFC4797: Use of Provider Edge to Provider Edge (PE-PE) Generic Routing Encapsulation (GRE) or IP in BGP/MPLS IP Virtual Private Networks
- RFC5158: 6to4 Reverse DNS Delegation Specification
- RFC5214: Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
- RFC5332: MPLS Multicast Encapsulations
- RFC5579: Transmission of IPv4 Packets over Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Interfaces
- RFC5845: Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6
- RFC5969: IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification
- RFC6245: Generic Routing Encapsulation (GRE) Key Extension for Mobile IPv4
- RFC6343: Advisory Guidelines for 6to4 Deployment
- draft-zhou-dhc-gre-option-00 DHCPv4 and DHCPv6 options for GRE
- draft-cai-softwire-6rd-mib-03 Definitions of Managed Objects for 6rd
- draft-howard-isp-ip6rdns-05 Reverse DNS in IPv6 for Internet Service Providers
- draft-tsou-softwire-6rd-multicast-02 IPv6 Multicast Using Native IPv4 Capabilities in a 6rd Deployment
- draft-templin-v6ops-isops-18 Operational Guidance for IPv6 Deployment in IPv4 Sites using ISATAP

6.2 Applications

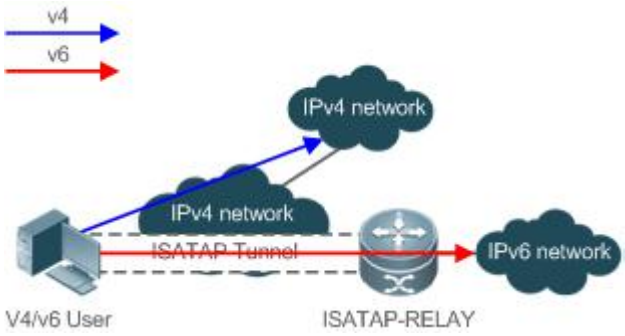
Application	Description
Accessing the IPv6 Sites on a Campus Network	Accesses the IPv6 sites on a campus network.
Connecting a Campus Network to an IPv6 Backbone Network	Connects a campus network to an IPv6 backbone network.

6.2.1 Accessing the IPv6 Sites on a Campus Network

Scenario

IPv6 servers are deployed on some campus networks, and PCs need to access the servers. The Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) can be used to realize the access.

Figure 6-1



Remarks	ISATAP-RELAY supports tunneling. Users on the campus network can access IPv4 servers directly through the IPv4 network,

	but need to access IPv6 servers through the ISATAP tunnel.

Deployment

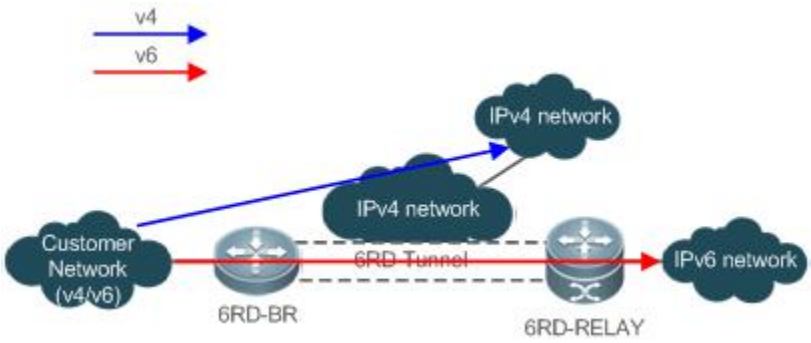
- IPv4 and IPv6 users access the IPv4 network by using IPv4 addresses.
- IPv4 and IPv6 users access the IPv6 network through the ISATAP tunnel.
- The ISATAP tunnel is established between PCs and the ISATAP-RELAY router.

6.2.2 Connecting a Campus Network to an IPv6 Backbone Network

Scenario

A campus network needs to be upgraded to support IPv6, or an IPv6 campus network needs to be built. Automatic 6RD and 6to4 tunnels can be used to meet the requirements.

Figure 6-2



Remarks	6RD-BR is a 6RD border router. 6RD-RELAY is a 6RD relay router. The customer network can access the IPv6 network through the 6RD tunnel across the IPv4 network.

Deployment

- A 6RD tunnel is established between the 6RD-BR and 6RD-RELAY routers.
- The 6RD tunnel is deployed by an Internet service provider (ISP).
- The configuration of the 6RD-BR router is obtained dynamically through the Dynamic Host Configuration Protocol (DHCP).

6.3 Features

Basic Concepts

Tunnel MTU

- The MTU of a tunnel interface is smaller than that of a regular interface, such as a regular IPv4 over IPv4 tunnel. The maximum amount of data carried by a packet transmitted over the Ethernet is 1,460 bytes, not including the two IP headers. Therefore, the MTU of a tunnel interface is 1,480 bytes, not 1,500 bytes of a standard Ethernet interface.

Tunnel Path MTU

- A tunnel interface represents a virtual link. For an IPv4 over IPv4 tunnel, the MTU of the tunnel interface is the MTU of the tunnel link, that is, the MTU of the path between the local and peer ends of the tunnel When the routing path between the local and peer ends is changed, the MTU of the path may also be changed, which will affect the MTU of the tunnel interface.

Tunnel Encapsulation Limit

- Tunnel encapsulation is supported. For example, an IPv4 packet can be encapsulated with two or more IPv4 headers and then transmitted in an IPv4 over IPv4 tunnel. Tunnel encapsulation is intended for security protection and used sparingly. The amount of data to be transmitted is reduced after tunnel encapsulation. After routing through the forwarding information base (FIB), if the outbound interface is another tunnel interface, tunnel encapsulation occurs. If the outbound interface is the local tunnel interface, infinite encapsulation occurs. (FS products can detect this case and give prompts.)

Overview

Feature	Description
Tunnel Reachability Detection	Checks whether tunnel links are available.
Tunnel MTU Auto-Adjustment	Dynamically adjusts the MTU of a tunnel interface based on the changes of the path MTU of the tunnel link.
Tunnel Encapsulation Limit	Increases the maximum number of nested encapsulations of a packet based on actual requirements. (This feature is rarely used.)
Tunnel Data Validity Check	Adds checksum to the data transmitted in GRE tunnels to check whether an error occurs during transmission.

6.4 Configuration

Configuration	Description and Command	
Configuring Tunnel Interfaces	(Mandatory) It is used to create tunnels.	
	Interface tunnel	Creates a tunnel interface.
	tunnel source	Configures the local address of a tunnel.
Configuring a Tunnel Mode	(Optional) It is used to configure a tunnel mode.	
	tunnel mode	Configures a tunnel encapsulation mode.
Configuring a Peer Address	(Optional) It is used to configure the peer address of a tunnel.	
	tunnel destination	Configures the peer address of a tunnel.
Configuring the TOS of a Tunnel	(Optional) It is used to configure the type of service (TOS) of a tunnel.	
	tunnel tos	Configures the TOS of a tunnel.
Configuring the TTL of a Tunnel	(Optional) It is used to configure the time to live (TTL) of a tunnel.	
	tunnel ttl	Configures the TTL of a tunnel.
Configuring Tunnel 6RD BR	(Optional) It is used to configure the BR IPv4 address of a tunnel.	
	tunnel 6rd br	Configures the BR IPv4 address of a 6RD tunnel.

Configuration	Description and Command	
Configuring Tunnel 6RD IPv4	(Optional) It is used to configure the length of the IPv4 general prefix and suffix.	
	tunnel 6rd ipv4	Configures the length of the IPv4 general prefix and suffix.
Configuring a Tunnel 6RD Prefix	(Mandatory) It is used to configure the IPv6 prefix of a tunnel.	
	tunnel 6rd br	Configures the IPv6 prefix of a 6RD tunnel.

6.4.1 Configuring Tunnel Interfaces

Configuration Effect

- Create a tunnel interface.

Configuration Steps

Creating a Tunnel Interface

- Run the **interface tunnel** *number* command in global configuration mode to create a tunnel interface.
- The tunneling service is available only after a tunnel interface is created.

Verification

- Run the **show interfaces tunnel** *number* command to check whether the tunnel interface is created successfully.

Related Commands

Configuring a Tunnel Interface

Command	**interface tunnel** *number*
Parameter Description	*number*: Indicates the number of a tunnel interface.
Command Mode	Global configuration mode
Usage Guide	N/A

Checking the Tunnel Configuration

Command	**show interfaces tunnel** *number*
Parameter Description	*number*: Indicates the number of a tunnel interface.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Creating a Tunnel Interface

Configuration Steps	● Create a tunnel interface.
	FS# configure terminal FS(config)# interface tunnel 1 FS(config-if-Tunnel 1)# end
Verification	● Check the configuration of the tunnel interface.
	FS# show interfaces tunnel 1 …… Tunnel attributes: …… Tunnel protocol/transport is gre ip

Common Errors

- A tunnel interface cannot be created due to memory deficiency.
- A tunnel interface cannot be created due to insufficient hardware resource deficiency.

6.4.2 Configuring a Tunnel Mode

Configuration Effect

- Configure a tunnel encapsulation mode in tunnel interface configuration mode when you need to use a tunnel in non-default encapsulation mode.

Configuration Steps

Configuring a Tunnel Mode

- Optional.
- The default encapsulation mode for routers and gateway products is tunnel mode gre ip.
- To change the default encapsulation mode, run the **tunnel mode** command in tunnel interface configuration mode.

Verification

- Run the **show interfaces tunnel** *number* command to check whether the tunnel encapsulation mode is configured.

Related Commands

Configuring a Tunnel Mode

Command	**tunnel mode** { **gre** {**ip** | **ipv6**} | **ipv6** | **ipip** | **ipv6ip** [**6rd** | **6to4** | **isatap**] }
Parameter Description	Each mode corresponds to different encapsulation format of the packets sent out by the tunnel interface. **gre ip** indicates that a packet is encapsulated with a GRE header and an IPv4 header in sequence and then is

	transmitted over a new IPv4 network. **gre ipv6** indicates that a packet is encapsulated with a GRE header and an IPv6 header in sequence and then is transmitted over a new IPv6 network. **ipv6** indicates that a packet sent out by the tunnel interface is encapsulated with an IPv6 header and then transmitted over a new IPv6 network. **ipip** indicates that the tunnel interface carries only IPv4 packets and a packet sent out by the tunnel interface is encapsulated with an IPv4 header and then transmitted over a new IPv4 network. **ipv6ip** indicates that the tunnel interface carries only IPv6 packets and a packet sent out by the tunnel interface is encapsulated with an IPv4 header and then transmitted over a new IPv4 network. The preceding tunnels are manual tunnels, whereas IPv6IP 6RD, 6to4, and ISATAP are automatic tunnels. During packet encapsulation, the destination IPv4 address is mapped from the destination IPv6 address.
Command Mode	Interface configuration mode
Usage Guide	Both ends of a tunnel must be configured with the same encapsulation mode. Otherwise, the tunnel cannot work.

Configuration Example

Configuring the IPv4 over IPv4 Encapsulation Mode

Configuration Steps	● Configure the IPv4 over IPv4 encapsulation mode on a tunnel interface.
	FS# configure terminal FS(config)# interface tunnel 1 FS(config-if-Tunnel 1)# tunnel mode ipip FS(config)# end
Verification	● Check the configuration of the tunnel interface.
	FS# show interfaces tunnel 1 …… Tunnel attributes: …… Tunnel protocol/transport is ipv6ip

Common Errors

- A 6to4 tunnel or ISATAP tunnel is configured for a virtual routing and forwarding (VRF) instance that is already configured with a 6to4/ISATAP tunnel.

6.4.3 Configuring a Local Address

Configuration Effect

- Configure the local address of a tunnel.

Notes

- The local address of a tunnel must match the transport protocol used by the tunnel. Otherwise, the tunnel interface will not be up (be disabled).
- When the local address is specified indirectly by configuring another interface, the local address is the primary IPv4 address or the first global public IPv6 address of IPv6.

Configuration Steps

Configuring a Local Address

- Mandatory.
- Run the **tunnel source** command in tunnel interface configuration mode to specify the local address of a tunnel.

Verification

- Run the **show interfaces tunnel** *number* command to display the local address of the tunnel.

Related Commands

Configuring a Local Address

Command	**tunnel source** { *ip-address* | *interface-name interface-number* }
Parameter Description	**ip-address**: Indicates an IPv4 or IPv6 address. *interface-name interface-number*: Indicates a Layer-3 interface.
Command Mode	Interface configuration mode
Usage Guide	If you specify an IPv4 or IPv6 address directly, you need to configure the address of the device.

Configuration Example

Configuring a Local Address

Configuration Steps	• Configure the local address of a tunnel as 1.1.1.1.
	FS# configure terminal FS(config)# interface tunnel 1 FS(config-if-Tunnel 1)# tunnel mode ipv6ip FS(config-if-Tunnel 1)# tunnel source 1.1.1.1
Verification	• Check the configuration of the tunnel interface.
	FS# show interfaces tunnel 1 …… Tunnel attributes:

	Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable Tunnel TOS/Traffic Class not set, Tunnel TTL 254 Tunnel config nested limit is 0, current nested number is 0 Tunnel protocol/transport ipv6ip Tunnel transport VPN is no set ……

6.4.4 Configuring a Peer Address

Configuration Effect

- A manual tunnel can be used (the tunnel interface is up) only after its peer address is configured.

Notes

- Peer addresses cannot be configured for automatic tunnels.

Configuration Steps

Configuring a Peer Address

- The peer addresses must be configured for all tunnels except 6RD, 6to4, and ISATAP tunnels.
- Run the **tunnel destination** command in interface configuration mode to configure the peer address of a tunnel.

Verification

- Run the **show interfaces tunnel** command to check whether the destination address is configured.

Related Commands

Configuring a Peer Address

Command	**tunnel destination** { *ip-address* }
Parameter Description	***ip-address***: Indicates an IPv4 or IPv6 address.
Command Mode	Interface configuration mode
Usage Guide	The peer address of a manual tunnel must be configured. The protocol suite type of the configured peer address must be consistent with the transport protocol used by the tunnel. If they are not consistent, the tunnel interface will be disabled (down).

Configuration Example

Configuring a Peer Address

Configuration Steps	• Configure the peer address of a tunnel as 2.2.2.2.

	FS# configure terminal FS(config)# interface tunnel 1 FS(config-if-Tunnel 1)# tunnel mode ipv6ip FS(config-if-Tunnel 1)# tunnel destination 2.2.2.2
Verification	● Check the configuration of the tunnel interface.
	FS# show interfaces tunnel 1 …… Tunnel attributes: Tunnel source: UNKNOWN, destination 2.2.2.2, unrouteable Tunnel TOS/Traffic Class not set, Tunnel TTL 254 Tunnel config nested limit is 0, current nested number is 0 Tunnel protocol/transport ipv6ip ……

Common Errors

- A peer address is configured for an automatic tunnel.
- The peer address configured for a tunnel is the same as that of another tunnel.
-

6.4.5 Configuring the TOS of a Tunnel

Configuration Effect

- Specify the TOS or Traffic Class field in the transport protocol header.

Notes

- If the TOS or Traffic Class field in the transport protocol header is not specified, the TOS or Traffic Class field of the protocol is copied to the header.

Configuration Steps

Configuring the TOS of a Tunnel

- Optional.
- To change the priority of tunnel data on a network, run the **tunnel tos** command in interface configuration mode.

Verification

- Run the **show interfaces tunnel** command to check whether the TOS is configured.

Related Commands

Configuring the TOS of a Tunnel

Command	**tunnel tos** *number*
Parameter Description	***number***: Indicates the TOS of a tunnel.
Command Mode	Interface configuration mode
Usage Guide	By default, if the IPv4 protocol is used for the inner bearer and outer encapsulation in a tunnel, the TOS bytes in the inner IPv4 header are copied to the outer IPv4 header. If the IPv6 protocol is used for the inner bearer and outer encapsulation in a tunnel, the Traffic Class 8 bit in the inner IPv6 header is copied to the outer IPv6 header. In other cases, the TOS field in the outer IPv4 header and the Traffic Class field in the IPv6 header are 0.

Configuration Example

Configuring the TOS of a Tunnel

Configuration Steps	● Configure the TOS of a tunnel.
	FS# configure terminal FS(config)# interface tunnel 1 FS(config-if-Tunnel 1)# tunnel mode ipv6ip FS(config-if-Tunnel 1)# tunnel tos 2
Verification	● Check the configuration of the tunnel interface.

	FS# show interfaces tunnel 1
	……
	Tunnel attributes:
	  Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable
	  Tunnel TOS/Traffic Class 0x2, Tunnel TTL 254
	  Tunnel config nested limit is 0, current nested number is 0
	  Tunnel protocol/transport ipv6ip
	  Tunnel transport VPN is VPN1
	……

6.4.6 Configuring the TTL of a Tunnel

Configuration Effect

- Specify the TTL or hop limit of tunnel encapsulation protocol headers.

Configuration Steps

Configuring the TTL of a Tunnel

- Optional.
- By default, the TTL is 254, which is the maximum value.
- To change the tunnel link length limit, run the **tunnel ttl** command.

Verification

- Run the **show interfaces tunnel** command to check whether the TTL is configured.

Related Commands

Configuring the TTL of a Tunnel

Command	**tunnel ttl** *hop-limit*
Parameter Description	*hop-limit*: Indicates the hop limit of a tunnel.
Command Mode	Global configuration mode
Usage Guide	The hop limit specifies the maximum number of routers that a packet can pass through. The default value is 255. This command is used to change the hop quantity limit.

Configuration Example

Configuring the TTL of a Tunnel

Configuration Steps	• Configure the TTL of a tunnel.
	FS# configure terminal FS(config)# interface tunnel 1 FS(config-if-Tunnel 1)# tunnel mode ipv6ip FS(config-if-Tunnel 1)# tunnel ttl 3
Verification	• Check the configuration of the tunnel interface.
	FS# show interfaces tunnel 1 …… Tunnel attributes: Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable Tunnel TOS/Traffic Class 0x2, Tunnel TTL 3 Tunnel config nested limit is 0, current nested number is 0 Tunnel protocol/transport ipv6ip Tunnel transport VPN is VPN1

6.4.7 Configuring Tunnel 6RD BR

Configuration Effect

- Configure the IPv4 address of a relay router of a 6RD tunnel.

Configuration Steps

Configuring a Relay Router of a Tunnel

- Optional.
- To configure the tunnel BR address, run the **tunnel 6rd br** *ipv4-address* command in tunnel interface configuration mode.

Verification

- Run the **show interfaces tunnel** command to check whether the tunnel BR address is configured.

Related Commands

Configuring a Tunnel BR Address

Command	**tunnel 6rd br** *ipv4-address*
Parameter Description	*ipv4-address*: Indicates the IP address of a relay router.
Command Mode	Interface configuration mode
Usage Guide	The tunnel calculates the destination IPv4 address based on the BR address, 6RD prefix, and 6RD IPv4 address.

Configuration Example

Configuring a Tunnel 6RD BR Address

Configuration Steps	• Configure a tunnel BR address.
	FS# configure terminal FS(config)# interface tunnel 100 FS(config-if-Tunnel 100)# ipv6 enable FS(config-if-Tunnel 100)# tunnel 6rd br 10.1.2.1
Verification	• Check the configuration of the tunnel interface.

Configuration Steps	● Configure a tunnel BR address.
	FS# configure terminal FS(config)# interface tunnel 100 FS(config-if-Tunnel 100)# ipv6 enable FS(config-if-Tunnel 100)# tunnel 6rd br 10.1.2.1
Verification	● Check the configuration of the tunnel interface.
	FS(config)#show int tunnel 1 …… Tunnel attributes: Tunnel source: UNKNOWN, destination UNKNOWN Tunnel TOS/Traffic Class not set, Tunnel protocol/transport ipv6ip 6rd 6rd prefix 0.0.0.0/0 Border relay 1.1.1.1 ……

6.4.8 Configuring Tunnel 6RD IPv4

Configuration Effect

- Configure the length of the IPv4 general prefix and suffix of a 6RD tunnel.

Notes

- **tunnel 6rd ipv4 prefix-length** *prefix-length* **suffix-length** *suffix-length* s used to configure the length of the prefix and suffix of the IPv4 address of a 6RD domain. The valid range of the value is 0–31. The total length of the prefix and suffix cannot exceed 31. The default length is 0.

Configuration Steps

Configuring the Length of the IPv4 General Prefix and Suffix of a 6RD Tunnel

- Optional.
- Run the **tunnel 6rd ipv4 prefix-length** *prefix-length* **suffix-length** *suffix-length* command in tunnel interface configuration mode.

Verification

- Run the **show interfaces tunnel** command to check the configuration.

Related Commands

Configuring the Length of the IPv4 General Prefix and Suffix of a 6RD Tunnel

Command	**tunnel 6rd ipv4 prefix-length** *prefix-length* **suffix-length** *suffix-length*
Parameter Description	*prefix-length*: Indicates the length of the prefix. *suffix-length:* Indicates the length of the suffix.
Command Mode	Interface configuration mode
Usage Guide	The tunnel calculates the destination IPv4 address based on the BR address, 6RD prefix, and 6RD IPv4 address.

Configuration Example

Configuring the Length of the IPv4 General Prefix and Suffix of a 6RD Tunnel

Configuration Steps	● Configure the length of the universal prefix and suffix of the 6RD IPv4 address of Tunnel 100.
	FS# configure terminal FS(config)# interface tunnel 100 FS(config-if-Tunnel 100)# ipv6 enable FS(config-if-Tunnel 100)# tunnel 6rd ipv4 prefix-length 8 suffix-length 8
Verification	● Check the configuration of the tunnel interface.

	FS#show int tunnel 1
	……
	Tunnel attributes:
	  Tunnel source: UNKNOWN, destination UNKNOWN
	  Tunnel TOS/Traffic Class not set,
	  Tunnel protocol/transport ipv6ip 6rd
	  6rd prefix 0.0.0.0/0
	  Border relay 1.1.1.1
	  ipv4 prefix-len 16, ipv4 suffix-len:8
	  Tunnel transport VPN is no set
	……

6.4.9 Configuring a Tunnel 6RD Prefix

Configuration Effect

- Configure the IPv6 prefix of a 6RD domain.

Notes

- The configuration is mandatory when 6RD is used. If no 6RD IPv6 prefix is configured, the 6RD tunnel cannot be up. If you set the prefix length to 0, no prefix will be configured.

Configuration Steps

Configuring the IPv6 Prefix of a 6RD Tunnel

- Optional.
- Run the **tunnel 6rd prefix** *ipv6-prefix prefix-length* command in tunnel interface configuration mode.

Verification

- Run the **show interfaces tunnel** command to check the configuration.

Related Commands

Configuring the IPv6 Prefix of a 6RD Tunnel

Command	**tunnel 6rd prefix** *ipv6-prefix prefix-length*
Parameter Description	*ipv6-prefix*: Indicates the 6RD IPv6 prefix. *prefix-length:* Indicates the length of the prefix.
Command Mode	Interface configuration mode
Usage Guide	The tunnel calculates the destination IPv4 address based on the BR address, 6RD prefix, and 6RD IPv4 address.

Configuration Example

Configuring the IPv6 Prefix of a 6RD Tunnel

Configuration Steps	• Configure the 6RD IPv6 prefix of Tunnel 100.
	FS# configure terminal FS# configure terminal FS(config)# interface tunnel 100 FS(config-if-Tunnel 100)# tunnel 6rd prefix 2001:da8::/32
Verification	• Check the configuration of the tunnel interface.
	FS#show int tunnel 1 …… Tunnel attributes: Tunnel source: UNKNOWN, destination UNKNOWN Tunnel TOS/Traffic Class not set, Tunnel protocol/transport ipv6ip 6rd

Configuration Steps	● Configure the 6RD IPv6 prefix of Tunnel 100.
	FS# configure terminal FS# configure terminal FS(config)# interface tunnel 100 FS(config-if-Tunnel 100)# tunnel 6rd prefix 2001:da8::/32
Verification	● Check the configuration of the tunnel interface.
	6rd prefix 32.1.0.0/64 Border relay 1.1.1.1 ipv4 prefix-len 16, ipv4 suffix-len:8 Tunnel transport VPN is no set ……

6.4.10 Configuring the IPsec Profile of a Tunnel

Configuration Effect

- After being encapsulated in a tunnel, data is encrypted through IPsec to improve security.

Configuration Steps

Configuring the IPsec Profile of a Tunnel

- Optional.
- Run the **crypto ipsec profile** *WORD* command in tunnel interface configuration mode.

Verification

- Run the **show run** command to check whether the IPsec profile is configured.

Related Commands

Creating an IPsec Profile

Command	**crypto ipsec profile** *WORD*
Parameter Description	*WORD*: Indicates the profile name.
Command Mode	Global configuration mode
Usage Guide	Run this command to create an IPsec profile for a tunnel so that the tunnel can be associated with the profile. Switches do not support the configuration of IPsec profile for tunnels.

Configuring the IPsec Profile of a Tunnel

Command	**tunnel protection ipsec profile** *WORD*
Parameter Description	*WORD*: Indicates the profile name.
Command Mode	Interface configuration mode
Usage Guide	Run this command to create an IPsec profile for a tunnel so that the tunnel can be associated with the profile.

Configuration Example

Configuring the IPsec Profile of a Tunnel

Configuration Steps	● Create an IPsec profile. FS# configure terminal FS(config)# crypto ipsec profile test ● Configure the IPsec profile of a tunnel.
	FS# configure terminal FS(config)# interface tunnel FS(config-if-Tunnel 1)# tunnel protection ipsec profile test
Verification	● Check the configuration of the tunnel interface.
	FS#show run int tunnel 1 Building configuration... Current configuration : 59 bytes ! interface Tunnel 1 tunnel protection ipsec profile test

6.5 Monitoring

Displaying

Description	Command
Displays the information about a tunnel interface.	**show interfaces tunnel** *number*

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Enables tunnel interface debugging.	**debug tunnel**

7 Configuring FPM

7.1 Overview

The flow platform (FPM) is a platform for the acceleration of packet service processing. Because IP packets have the flow attribute, the FPM provides services with the function to identify the flow attribute of IP packets before service processing, so as to improve service processing efficiency. The FPM is a fundamental platform. It is loaded upon system startup. The configuration commands described in this document are provided to implement FPM configuration and management. In general, the default configuration of the FPM can already meet practical requirements.

The following sections describe the FPM only.

Protocols and Standards

N/A

7.2 Applications

Application	Description
Configuring the packet receiving threshold	A standalone device serves as the gateway to forward packets.
Configuring loose TCP status check	Perform active/standby switchover in the AS environment.

7.2.1 Configuring the Packet Receiving Threshold

Scenario

When the device receives a large number of repeated TCP connection requests in a local area network (LAN), no legitimate connection can be established if the device cannot receive any handshake response packet from the peer. In this case, attacks probably occur. You can perform FPM configuration to restrict the number of TCP connection requests, so as to effectively defend against such attacks.

Protocols

- Enable the strict packet status tracing function on the forwarding device.
- Configure a low TCP-SYN-SENT packet threshold.

7.2.2 Configuring Loose TCP Status Check

Scenario

Loose TCP status check should be configured on the device to prevent flow interruption during active/standby switchover of the device. Then a connection can be established and packets can be forwarded as long as one end sends an ACK packet, so that the connection is not interrupted at all during the active/standby switchover.

Protocols

- Configure loose TCP status check on the backup device.

Basic Concepts

Flow Entry

A flow entry, as a physical resource for the device to identify and manage all connections of an IP session, records basic information about the current IP session. The corresponding protocols include ICMP, TCP, UDP, and RAWIP.

7.3 Features

Overview

Feature	Description
Transparent transmission when the flow table is full	This feature ensures that the existing flows are not interrupted when the flow table is full.
Flow entry aging	This feature reclaims invalid flow entries.
Number of packets permitted in a flow	This feature prevents IP packet flooding attacks.
TCP status tracing	This feature filters out packets on illegitimate TCP connections.
Strict packet status tracing	This feature performs packet threshold check.
Loose TCP status check	This feature allows the establishment of a connection with only ACK packets.

7.3.1 Transparent Transmission of Packets When the Flow Table Is Full

Working Principle

The acceleration of IP service processing relies on a flow table. Flow table resources are configured according to the current product hardware configuration and generally can meet application requirements in an application environment. In some extreme environments, however, flow table resources could be exhausted, causing the failure to establish flows. With this feature, packets are transparently transmitted instead of establishing any flow on wireless products when the flow table is full, and service processing is not accelerated, thereby ensuring that service flows are not interrupted.

7.3.2 Flow Entry Aging

Working Principle

The aging of a flow entry means that the device actively withdraws the flow entry when there is no data exchange in a certain period of time. If a session attack occurs, the flow table will be full, causing the failure to establish sessions. The aging of the flow table is designed to solve this problem. For flow entries of different data types, their aging time shall be set according to actual service requirements. For flows of different service data types, different aging time shall be set according to different states of the flows. For example, the aging time of a TCP flow in SYN status is different from that of a TCP flow in ESTABLISH status. For example again, when a port scanning attack occurs on a network, abundant flow table resources of the system are occupied, and then appropriate aging time can be configured for flows established on these connections according to the states of the flows, so as to effectively reclaim flow entries and avoid flow interruption. Configuring appropriate aging time can help to reduce "useless" flow entries in the flow table while meeting the requirement for exchanging service data flows.

7.3.3 Number of Packets Permitted in a Flow

Working Principle

For each flow in the current status, there is a counter that records the number of packets processed in the flow. An attacker may send a large number of packets of a certain type to wage a traffic attack, in which case other types of packets cannot be processed in time. You can configure the number of packets permitted to pass in a flow in a certain status, so as to solve this problem and meet the requirement for exchanging service data flows.

7.3.4 TCP Status Tracing

Working Principle

A complete handshake process is required for the establishment of a TCP connection; otherwise, the connection is illegitimate or the packets are attack packets. The FPM needs to trace the states of TCP connections, so as to distinguish flows that are established over TCP session connections in various states and determine whether the connections are legitimate. In some special scenarios such as asymmetrical routing, however, the states of TCP connections cannot be traced and then this function should be disabled.

7.3.5 Packet Threshold for Flows in Various States

Working Principle

For a flow in a certain status established over a connection, there is an upper limit on the number of packets permitted on the legitimate connection. If this upper limit is exceeded, a packet flooding attack probably occurs, occupying the forwarding resources of the system. Therefore, you can configure a packet threshold for flows in various states so as to effectively defend against such attacks.

7.3.6 Loose TCP Status Check

Working Principle

A complete handshake process is required for the establishment of a legitimate TCP connection. In some cases such as active/standby switchover, however, probably a handshake process has been performed for the current TCP connection but only no corresponding information exists. In such cases, the system requires only ACK packets. For this purpose, the FPM provides loose TCP status check.

7.4 Configuration

Configuration	Description and Command	
Configuring the Functions of the FPM	(Optional) It is used to manage FPM.	
	Ip session direct-trans-disable	Disables the function to transparently transmit packets when the flow table is full.
	ip session timeout	Configures the flow entry aging time.
	ip session threshold	Configures the number of packets that can be received for each flow in a certain status.
	ip session tcp_state-inspection-disable	Disables the TCP status tracing function.
	ip session tcp_state-inspection-enable	Enables the TCP status tracing function.

	ip session track-state-strictly	Configures packet threshold for flows in various states.
	ip session tcp-loose	Enables the loose TCP status transition check function.

7.4.1 Disabling Transparent Transmission of Packets When the Flow Table Is Full

Networking Requirements

- For some special services such as network address translation (NAT) applied on wireless products, the FPM should not allow the transparent transmission of packets without flow establishment.

Notes

- Currently this function is available on wireless products only.
- By default, packets can be transparently transmitted without flow establishment when the flow table is full.

Configuration Steps

- Optional configuration.
- By default, packets can be transparently transmitted without flow establishment when the flow table is full. You can use the **ip session direct-trans-disable** command to disable the function.

Command	**ip session direct-trans-disable**
Parameter Description	
Defaults	Packets can be transparently transmitted without flow establishment when the flow table is full.
Command Mode	Global configuration mode
Usage Guide	Use the **no** form of this command to enable the transparent transmission function.

Verification

- Use the **show run** command to check whether the configuration includes **ip session direct-trans-disable**. If no, the transparent transmission function is enabled.

Configuration Example

Scenario	If the NAT service is required on the current wireless device, you need to disable the transparent transmission function because the NAT service does not allow the transparent transmission of IP packets without flow establishment.
Configuration Steps	Disable transparent transmission of packets without flow establishment when the flow table is full.
	FS# configure terminal FS(config)# ip session direct-trans-disable
Verification	Use the **show run** command to verify that the configuration includes **ip session direct-trans-disable**.

Common Errors

N/A

7.4.2 Configuring the Flow Entry Aging Time

Networking Requirements

- Reasonably make use of system flow table resources so as to reduce "useless" flow entries in the flow table and meet the requirement for exchanging service data flows.

Notes

- There is a default aging time upon system initialization, which can meet practical requirements in most scenarios. Therefore, the configuration is optional.
- Because a certain time is required before the system detects the corresponding flow, the actual aging time is slightly later than the configured aging time.

Configuration Steps

Configuring the Aging Time

- Optional configuration.
- By default, a flow entry ages within the default aging time. If the default aging time does not meet the requirement, you can use the **ip session timeout** command to change it. The longer the aging time, the longer the time-to-live (TTL) of the flow entry.
- Perform this configuration on the corresponding forwarding device.

Command	**ip session timeout** {**icmp-closed** | **icmp-connected** | **icmp-started** | **rawip-closed** | **rawip-connected** | **rawip-established** | **rawip-started** | **tcp-close-wait** | **tcp-closed** | **tcp-established** | **tcp-fin-wait1** | **tcp-fin-wait2** | **tcp-syn-receive** | **tcp-syn-sent** | **tcp-syn-sent2** | **tcp-time-wait** | **udp-closed** | **udp-started** | **udp-connected** | **udp-established**} { *num* }
Parameter Description	**icmp-closed**: Sets the aging time of ICMP flows in closed status, which is 10 seconds by default and ranges from 5 to 60. **icmp-connected**: Sets the aging time of ICMP flows in connected status, which is 10 seconds by default and ranges from 5 to 120. **icmp-started**: Sets the aging time of ICMP flows in started status, which is 10 seconds by default and ranges from 5 to 120. **rawip-closed**: Sets the aging time of RAWIP flows in closed status, which is 10 seconds by default and ranges from 5 to 60. **rawip-connected**: Sets the aging time of RAWIP flows in connected status, which is 300 seconds by default and ranges from 10 to 300. **rawip-established**: Sets the aging time of RAWIP flows in established status, which is 300 seconds by default and ranges from 10 to 600. **rawip-started**: Sets the aging time of RAWIP flows in started status, which is 300 seconds by default and ranges from 10 to 300. **tcp-close-wait**: Sets the aging time of TCP flows in tcp-close-wait status, which is 60 seconds by default and ranges from 10 to 120.

	tcp-closed: Sets the aging time of TCP flows in tcp-closed status, which is 10 seconds by default and ranges from 5 to 20. **tcp-established**: Sets the aging time of TCP flows in tcp-established status, which is 1,800 seconds by default and ranges from 300 to 604,800. **tcp-fin-wait1**: Sets the aging time of TCP flows in tcp-fin-wait1status, which is 60 seconds by default and ranges from 10 to 120. **tcp-fin-wait2**: Sets the aging time of TCP flows in tcp-fin-wait2status, which is 60 seconds by default and ranges from 10 to 120. **tcp-syn-sent**: Sets the aging time of TCP flows in tcp-syn-sent status, which is 10 seconds by default and ranges from 5 to 30. **tcp-syn_sent2**: Sets the aging time of TCP flows in tcp-syn_sent2 status, which is 10 seconds by default and ranges from 5 to 30. **tcp-syn-receive**: Sets the aging time of TCP flows in tcp-syn-receive status, which is 10 seconds by default and ranges from 5 to 30. **tcp-time-wait**: Sets the aging time of TCP flows in tcp-time-wait status, which is 10 seconds by default and ranges from 5 to 60. **udp-closed**: Sets the aging time of UDP flows in closed status, which is 10 seconds by default and ranges from 5 to 60. **udp-connected**: Sets the aging time of UDP flows in connected status, which is 30 seconds by default and ranges from 10 to 300. **udp-established**: Sets the aging time of UDP flows in established status, which is 600 seconds by default and ranges from 120 to 600. **udp-started**: Sets the aging time of UDP flows in started status, which is 10 seconds by default and ranges from 10 to 300. **num**: Sets the aging time
Defaults	Default values apply.
Command Mode	Global configuration mode
Usage Guide	Use the **no** form of the commands to restore the default aging time.

Verification

- Use the **show run** command to check whether the configuration includes **ip session timeout**. If no, the default aging time applies.

Configuration Example

Scenario	If there are a large number of UDP-established flows which occupy a great space of the flow table on the current forwarding device, you can shorten the aging time of the UDP-established flows to improve aging efficiency.
Configuration Steps	The current forwarding device is a FW card located in slot 2 of device 1. Set the aging time of flows in udp-established status to 120 seconds.
	FS# configure terminal FS(config)# ip session 1 2 timeout udp-established 120
Verification	Check the aging time of flows in udp-established status on the device in slot 2 of device 1. The aging time should be 120 seconds. Use the **show run** command to verify that the configuration contains the following item:

	ip session 1 2 timeout udp-established 120 This indicates that the aging time is 120 seconds.

Common Errors

-

7.4.3 Configuring the Number of Packets Permitted in a Flow

Networking Requirements

- An attacker may send a large number of packets of a certain type to wage a traffic attack, in which case other types of packets cannot be processed in time. You can configure the number of packets permitted in a flow in a certain status, so as to solve this problem and meet the requirement for exchanging service data flows.

Notes

- There is a default packet count upon system initialization, which can meet practical requirements in most scenarios. Therefore, the configuration is optional.
- The check function here is disabled by default. To enable the check function, you need to configure packet threshold check for flows in various states first.

Configuration Steps

- Optional configuration.
- By default, a flow is judged according to the default number of packets permitted to pass in the flow. If the default number of packets permitted to pass does not meet the requirement, you can use the **ip session threshold** command to change the number of packets allowed to pass in the corresponding flow. The greater the value, the more packets permitted to pass in the flow.
- Perform this configuration on each forwarding device as necessary.

Command	**ip session threshold** {icmp-closed | **icmp-started** | rawip-closed | **tcp-syn-sent | tcp-syn-receive** | **tcp-closed | udp-closed** } { *num* }
Parameter Description	**icmp-closed**: Sets the number of packets permitted to pass in each ICMP flow in closed status, which is 10 by default and ranges from 1 to 2,000,000,000. **icmp-started**: Sets the number of packets permitted to pass in each ICMP flow in started status, which is 300 by default and ranges from 5 to 2,000,000,000. **rawip-closed**: Sets the number of packets permitted to pass in each RAWIP flow in closed status, which is 10 by default and ranges from 1 to 2,000,000,000. **tcp-syn-sent**: Sets the number of packets permitted to pass in each TCP flow in syn-send status, which is 10 by default and ranges from 10 to 2,000,000,000. **tcp-syn-receive**: Sets the number of packets permitted to pass in each TCP flow in syn-receive status, which is 20 by default and ranges from 5 to 2,000,000,000. **tcp-closed**: Sets the number of packets permitted to pass in each TCP flow in closed status, which is 20 by default and ranges from 5 to 2,000,000,000. **udp-closed**: Sets the number of packets permitted to pass in each UDP flow in closed status, which is 10 by default and ranges from 1 to 2,000,000,000. *num*: Sets the number of packets permitted to pass

Command Mode	Global configuration mode
Usage Guide	Use the **no** form of the command to restore the default number of packets permitted to pass.

Verification

- Use the **show run** command to check whether the configuration includes **ip session threshold**. If no, the default values about the number of packets permitted to pass apply.

Configuration Example

Scenario	When a large number of ping packets exist on a network, a flooding attack probably occurs. You can configure the number of packets permitted to pass in each ICMP flow in icmp-started status, so as to deny such ping packets.
Configuration Steps	The current forwarding device is a FW card located in slot 2 of device 1. Set the number of packets permitted to pass in each ICMP flow in icmp-started status to 10.
	FS# configure terminal FS(config)# ip session threshold icmp-started 10
Verification	On the device in slot 2 of device 1, check configuration information about the number of packets permitted to pass in each ICMP flow in icmp-started status. The number should be 10. Use the **show run** command to verify that the configuration contains the following item: ip session threshold icmp-started 10 This indicates that the number of packets permitted to pass in each ICMP flow in icmp-started status is 10.

Common Errors

-

7.4.4 Disabling the TCP Status Tracing Function

Networking Requirements

- In some special scenarios such as asymmetrical routing, the states of TCP connections cannot be traced. Perform this configuration to disable the TCP status tracing function.

Notes

- After the TCP status tracing function is disabled, the FPM will operate in abnormal status and then some services or features based on the status transition function of the FPM may fail to operate. Therefore, exercise caution with this configuration.
- The TCP status tracing function is enabled by default.

Configuration Steps

- Optional configuration.
- The TCP status tracing function is enabled by default. You can use the **ip session tcp-state-inspection-disable** command to disable the TCP status tracing function.
- If the TCP status tracing function needs to be disabled in a scenario such as asymmetrical routing, disable the TCP status tracing on each forwarding device as necessary.

Command	**ip session tcp-state-inspection-disable**

Parameter Description	N/A
Defaults	The TCP status tracing function is enabled.
Command Mode	Global configuration mode
Usage Guide	Use the **no** form of this command to restore the TCP status tracing function to default.

Verification

- Use the **show run** command to check whether the configuration includes **ip session tcp-state-inspection-disable**. If no, the TCP status tracing function is enabled.

Configuration Example

Scenario	The current forwarding device is a FW card located in slot 2 of device 1. If the FW card is located on an asymmetrical routing path in the current forwarding environment, you need to disable the TCP status tracing function.
Configuration Steps	Disable the TCP status tracing function on the forwarding device in slot 2 of device 1.
	FS# configure terminal FS(config)# ip session tcp-state-inspection-disable
Verification	Use the **show run** command to verify that the configuration includes **ip session tcp-state-inspection-disable**.

Common Errors

-

7.4.5 Enabling the TCP Status Tracing Function

Networking Requirements

- The TCP status tracing function needs to be enabled on corresponding wireless products.

Notes

- By default, the TCP status tracing function is disabled on wireless products.

Configuration Steps

- Optional configuration.
- By default, the TCP status tracing function is disabled on wireless products. You can use the **ip session tcp-state-inspection-enable** command to enable the TCP status tracing function.

Command	**ip session tcp-state-inspection-enable**
Parameter Description	
Defaults	The TCP status tracing function is disabled.
Command Mode	Global configuration mode
Usage Guide	Use the **no** form of this command to restore the TCP status tracing function to the default.

Verification

- Use the **show run** command to check whether the configuration includes **ip session tcp-state-inspection-enable**. If no, the TCP status tracing function is disabled.

Configuration Example

Scenario	The TCP status tracing function needs to be enabled on the current wireless forwarding device.
Configuration Steps	Enable the TCP status tracing function on the device.
	FS# configure terminal FS(config)# ip session tcp-state-inspection-enable
Verification	Use the **show run** command to verify that the configuration includes **ip session tcp-state-inspection-enable**.

Common Errors

-

7.4.6 Configuring Packet Threshold Check for Flows in Various States

Networking Requirements

- Perform this configuration to enable the packet threshold check function and disable the current flow when packets are unreachable.

Notes

-

Configuration Steps

- Optional configuration.
- You can use the **ip session track-state-strictly** command to enable the strict packet status tracing function.
- The packet threshold check function needs to be enabled in a scenario such as the scenario where attacks are waged using a certain type of packet.

Command	**ip session track-state-strictly**
Parameter Description	N/A
Defaults	The strict packet status tracing function is disabled.
Command Mode	Global configuration mode
Usage Guide	Use the **no** form of this command to restore the default configuration.

Verification

- Use the **show run** command to check whether the configuration includes **ip session track-state-strictly**. If no, the strict packet status tracing function is disabled.

Configuration Example

Scenario	If ICMP flooding attacks occur in the current network environment, packet threshold check is needed. In this case, perform this configuration to enable the packet threshold check function.
Configuration Steps	The current forwarding device is a FW card located in slot 2 of device 1. Enable the strict packet status tracing function on the forwarding device.
	FS# configure terminal FS(config)# ip session track-state-strictly
Verification	Use the **show run** command to verify that the configuration includes **ip session track-state-strictly**.

Common Errors

-

7.4.7 Configuring Loose TCP Status Check

Networking Requirements

- A flow can be directly established with only ACK packets.

Notes

- By default, the establishment of a flow with an ACK packet is not allowed on FW products but enabled on EG products.
- This configuration is optional.

Configuration Steps

- Optional configuration.
- By default, the loose TCP status check function is disabled on FW products. You can use the **ip session tcp-loose** command to enable the loose TCP status check function. By default, the loose TCP status check function is enabled on all wireless and EG products.
- The loose TCP status check function is required on the standby device in a scenario such as active/standby switchover.

Command	**ip session tcp-loose**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use the **no** form of this command to restore the default configuration.

Verification

- Use the **show run** command to check whether the configuration includes **ip session tcp-loose**. If no, the loose TCP status check function is disabled.

Configuration Example

Scenario	The current forwarding device is a FW card located in slot 2 of device 1. Active/standby switchover is required in the current environment. Perform this configuration on the backup device.

Configuration Steps	Enable the loose TCP status check function on the device in slot 2 of device 1.
	FS# configure terminal FS(config)# ip session tcp-loose
Verification	Use the **show run** command to verify that the configuration includes **ip session tcp-loose**.

Common Errors

-

7.5 Monitoring

Clearing

If you run the **clear** command while the device is operating, services may be interrupted arising from the loss of important information.

Function	Command
Clears counters about the IPv4 packets.	**clear ip fpm counters**

Displaying

Function	Command
Displays the counters about the IPv4 packets	**show ip fpm**
Displays IPv4 packet flow information	**show ip fpm**
Displays IPv4 flow statistics	**show ip fpm statistics**

8 Configuring NAT

8.1 Overview

Network Address Translation (NAT) is a process of translating the IP address in the header of an IP data packet into another IP address. In practice, NAT enables private networks that use unregistered IP addresses to access public networks. This way of using a small number of public IP addresses to represent substantial private IP addresses implements IP address conservation.

Protocols and Standards

- RFC 1631: The IP Network Address Translator (NAT)
- RFC 2663: IP Network Address Translator (NAT) Terminology and Considerations
- RFC 2391: Load Sharing using IP Network Address Translation (LSNAT)
- RFC 4008: Definitions of Managed Objects for Network Address Translators (NAT)

8.2 Applications

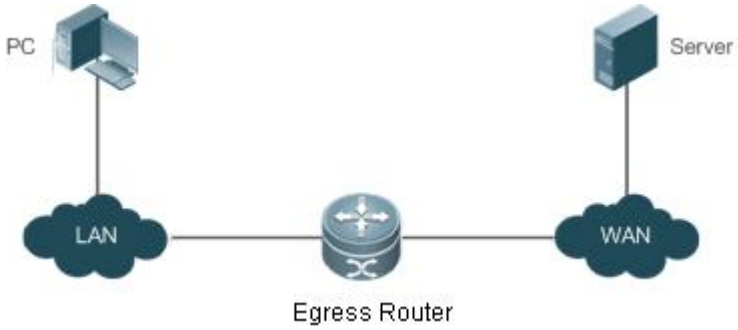
Application	Description
Intranet Users' Access to the Internet	NAT allows an intranet to communicate with the Internet by translating an inside private IP address into a globally unique IP address.
External Users' Access to an Intranet Server	NAT allows external networks to access internal devices by mapping one or more internal hosts to a network server.
Source/Destination Address Translation for Internal Users	When two private networks to interconnect with each other are configured with the same IP address or the same global IP address is allocated to both a private network and a public network, the two network hosts with the same IP address cannot communicate. NAT allows overlapping networks to communicate.
Intranet Server Load Balancing	When the TCP traffic load of an intranet host is excessively heavy, multiple hosts are deployed for TCP service load balancing. In this case, NAT may be used to attain this objective.

8.2.1 Intranet Users' Access to the Internet

Scenario

A PC is located in an intranet while a server is located in an extranet, as shown in Figure 7-1. In view of IP address depletion, only one or a few public IP addresses are allocated to the entire campus network. An egress router belongs to the intranet, and connects to the extranet. The basic NAT function is required on the egress router to allow the intranet PC to access the extranet server.

Figure 8-1



The egress router connects both the intranet and the extranet.

Corresponding Protocols

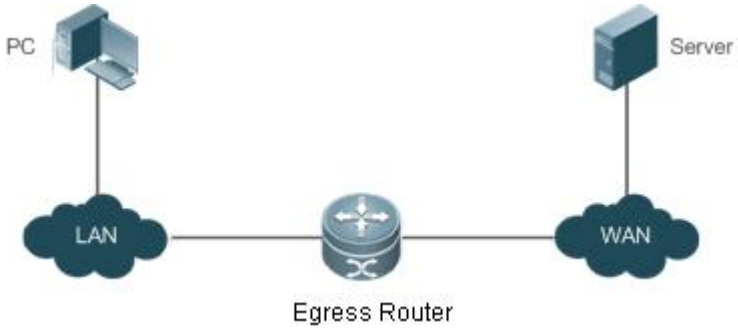
- Configure an inside interface and an outside interface for NAT.
- Configure static inside source address translation on the egress router.

8.2.2 External Users' Access to an Intranet Server

Scenario

A PC is located in an extranet while a server (such as a Web server) is located in an intranet, as shown in Figure 7-2. In view of IP address depletion, only one public IP address is allocated to the entire campus network. An egress router belongs to the intranet, and connects to the extranet. The Network Address and Port Translation (NAPT) function is required on the egress router to enable the PC to access the intranet server; that is, port mapping applies to the Web service port.

Figure 8-2



The egress router connects both the intranet and the extranet.

The server is deployed in the intranet.

Corresponding Protocols

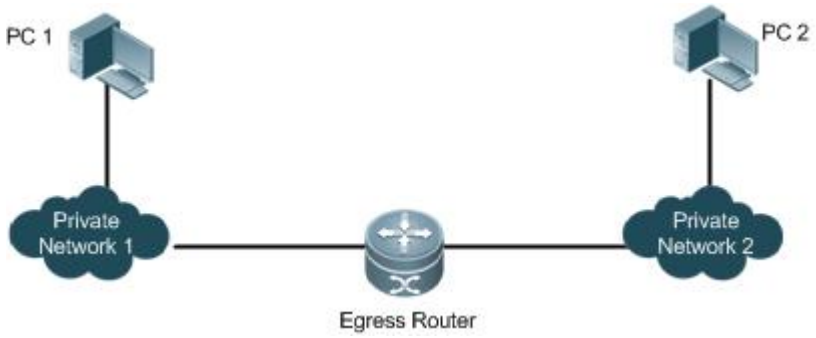
- Configure an inside interface and an outside interface for NAT.
- Configure server port address translation rules on the egress router.

8.2.3 Source/Destination Address Translation for Internal Users

Scenario

PC 1 is located in private network 1 while PC 2 is located in private network 2, as shown in Figure 7-3. Because the two private networks are separately managed, address overlapping occurs in their IP network segments. For example, the IP addresses of PC 1 and PC 2 are configured in the same network segment 192.168.1.0/24. An egress router is located between private networks 1 and 2. The NAT function needs to be enabled on the egress router, so that PC 1 and PC 2 can access each other.

Figure 8-3



The egress router connects both private networks.

Corresponding Protocols

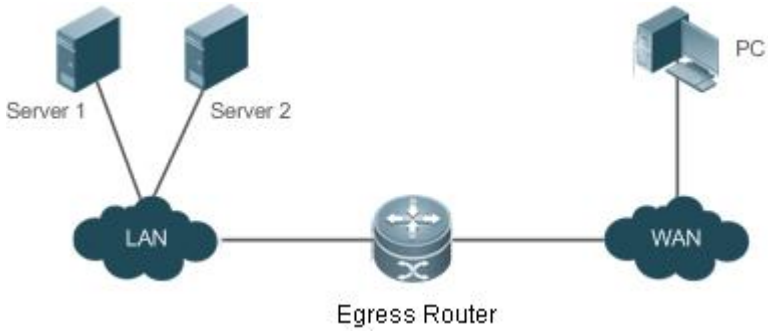
- Configure an inside interface and an outside interface for NAT.
- Configure dynamic translation of the inside source address on the egress router.
- Configure dynamic translation of the outside source address on the egress router.

8.2.4 Intranet Server Load Balancing

Scenario

Server 1 and Server 2 are located in an intranet, and form a cluster, as shown in Figure 7-4. A PC is located in an extranet. In view of IP address depletion, only one public IP address is allocated to the entire campus network. An egress router belongs to the intranet, and connects to the extranet. The egress router needs to distribute the server access traffic of the external user to the two servers; therefore, the NAT load balancing function needs to be enabled on the egress router.

Figure 8- 4



The egress router connects both the intranet and the extranet.

The servers are deployed in the intranet.

Corresponding Protocols

- Configure an inside interface and an outside interface for NAT.

- Configure TCP load balancing using NAT on the egress router.

8.3 Features

Basic Concepts

Private Address and Public Address

A private address is the IP address of an intranet or an intranet host, whereas a public address is an IP address globally unique on the Internet. The Internet Assigned Numbers Authority (IANA) has stipulated the following IP addresses for use on private networks, which cannot be allocated for use on the Internet but can be used inside any institution or corporation.

Class A private addresses: 10.0.0.0 to 10.255.255.255

Class B private addresses: 172.16.0.0 to 172.31.255.255

Class C private addresses: 192.168.0.0 to 192.168.255.255

NAT was initially designed to enable a private network to access a public network. Later it was extended to implement address translation for mutual access between any two networks. In this document, the two networks are called an intranet and an extranet. In general, a private network is an intranet, and a public network is an extranet.

Static NAT

Static NAT allows one-to-one permanent mappings between inside local addresses and inside global addresses. Static NAT is important when an extranet needs to access internal hosts via a fixed global routable address.

Dynamic NAT

Dynamic NAT establishes temporary mapping relationships between inside local addresses and inside global addresses. The temporary mapping relationships will be removed when unused in a certain period of time. Dynamic NAT can be configured in the following case: An intranet accesses extranet services only but does not provide services, and the number of intranet hosts is greater than the number of global IP addresses.

Overview

Feature	Description
Basic NAT	This feature translates inside private addresses into globally unique addresses, so that the intranet and the public network can communicate with each other.
NAPT	This feature maps multiple inside local addresses to one inside global address, so as to resolve the problem of IP address depletion.
Overlapping NAT	This feature enables overlapping networks to communicate.
TCP Load Balancing	This feature resolves the problem of TCP traffic overload.
Constructing a Local Server	This feature enables extranet to access the local server.
ALG	NAT changes only the header of an IP packet but not the payload of a specific application protocol. Therefore, the Application Level Gateway (ALG) is introduced to support application layer protocols.

8.3.1 Basic NAT

NAT is required for an intranet to communicate with an extranet by translating an inside private IP address into a globally unique IP address. You can configure static or dynamic NAT or both to implement interconnection and interworking.

Working Principle

An IP packet sent by an intranet host (192.168.1.2) to an extranet server (8.8.8.8) reaches an NAT device.

The NAT device checks the content of the IP packet, and finds that the IP packet is destined to an extranet. Therefore, the NAT device translates the private IP address 192.168.1.2 in the source IP address field of the IP packet into a public IP address 30.1.1.1 routable on the Internet, sends the IP packet to the extranet server, and at the same time records the mapping in its own NAT table.

The extranet server returns a response packet (in which the initial destination IP address is 30.1.1.1) to the intranet user. When the response packet reaches the NAT device, the NAT device checks the content of the response packet, looks up the mapping record in the NAT table, and replaces the initial destination IP address with the inside private IP address 192.168.1.2.

The above NAT process is transparent to terminals, such as the host and the server shown in the preceding figures. In the point of view of the extranet server, the IP address of the intranet host is 30.1.1.1 and the extranet server itself does not know the existence of the IP address 192.168.1.2 at all. Therefore, NAT "hides" the private network of an enterprise.

Basic NAT includes static NAT and dynamic NAT.

Related Configuration

Configuring NAT Interfaces

- An interface is not an NAT interface by default.
- Run the **ip nat { inside | outside }** command to specify a pair of NAT interfaces.
- NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured.

Configuring Static NAT

- Static NAT is not configured by default.
- Use the **ip nat inside source static** *local-address global-address* [**permit-inside**] [**netmask** *mask*] [**match** *interface*] [**description** *description-text*] command to configure static one-to-one NAT mapping.

Configuring Dynamic NAT

- Dynamic NAT is not configured by default.
- Use the **ip nat inside source list** *access-list-number* **pool** *address-pool* [**description** *description-text*] command to configure dynamic NAT mapping.

8.3.2 NAPT

In general, traditional NAT is one-to-one address mapping, which, however, cannot meet the requirements of all hosts in intranets to communicate with extranets. For example, when the intranet is in short of global IP addresses or even does not apply for global IP addresses but has only one global IP address to connect to an Internet Service Provider (ISP) while a large number of hosts in the intranet need to access the Internet, NAPT is required in this scenario.

Multiple inside local addresses can map to one inside global address using NAPT.

Working Principle

NAPT, also known as multiple-to-one address translation, allows multiple inside addresses to map to one public address. NAPT maps both IP addresses and port numbers; that is, the source addresses of data packets from different inside addresses can map to the same public address, but their port numbers are translated into different port numbers of the public address so that the same address can still be shared. NAPT is translation between "private IP address + Port number" and "Public IP address + Port number".

Static NAPT

In general, static NAPT is used to map the specified port on a specified host in an intranet to the specified port of a global address. In comparison, as mentioned previously, static NAT maps an internal host to a global address. Static NAPT is applicable to intranet hosts that provide the information service. Static NAPT provides a permanent one-to-one "IP address + Port" mapping relationship.

Dynamic NAPT

Dynamic NAPT is applicable to intranet hosts that only access extranet services but do not provide any information service. Dynamic NAPT provides a temporary one-to-one "IP address + Port" mapping relationship.

Related Configuration

Configuring NAT Interfaces

- An interface is not an NAT interface by default.
- run the **ip nat { inside | outside }** command to specify a pair of NAT interfaces.
- NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured.

Configuring Static NAPT

- Static NAPT is not configured by default.
- Use the **ip nat inside source static** local-ip local-port global-ip global-port [permit-inside] [**description** *description-text*] command to configure static one-to-one NAPT mapping.

Configuring Dynamic NAPT

- Dynamic NAPT is not configured by default.
- Use the **ip nat inside source list** *access-list-number* { [**pool** *address-pool*] | [**interface***interface-type interface-number*] } **overload** [**description** *description-text*] command to configure dynamic NAPT mapping. For NAPT, generally only one IP address is defined in the address pool, and one IP address supports up to 64,512 times of NAT. If one IP address is not enough, multiple IP addresses can be defined in the address pool.

8.3.3 Overlapping NAT

When the same IP address is allocated to two private networks to interconnect with each other or the same global IP address is allocated to a private network and a public network, this situation is called address overlapping. Two overlapping network hosts cannot communicate, because both hosts consider that the peer host is in the local network. Overlapping NAT is especially designed to implement the communications between two networks with the same IP address. After overlapping NAT is configured, an extranet host address will be represented as another host address in the intranet, and vice versa.

Working Principle

For mutual access between an intranet and an extranet with the same IP address, NAT needs to translate the inside address into a unique outside address. In addition, NAT needs to translate the outside address that overlaps with the inside address into another unique inside address.

Related Configuration

Configuring NAT Interfaces

- An interface is not an NAT interface by default.
- run the **ip nat { inside | outside }** command to specify a pair of NAT interfaces.
- NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured.

Configuring Inside Source Address Translation

- Inside source address translation is not configured by default.
- Static/dynamic basic NAT or static/dynamic NAPT can be used for inside source address translation. For details, see the "Basic NAT" and "NAPT" sections.

Configuring Static Translation of Outside Source Address

- Static translation of outside source address is not configured by default.
- Use the **ip nat outside source static** *global-address local-address* command to configure static translation of outside source address.

Configuring Dynamic Translation of Outside Source Address

- Dynamic translation of outside source address is not configured by default.
- Use the **ip nat outside source list** *access-list-number* **pool** *address-pool* command to configure dynamic translation of outside source address.

Configuring an ACL

- No ACL is configured by default.
- Use the **ip access-list { extended | standard } {** *id* | *name* **}** command or the **access-list** command to configure an ACL.

Configuring a Static Route

- Mandatory configuration.
- Use the **ip route** *network net-mask* { *ip-address* | *interface* [*ip-address*] } [*distance*] [**tag** *tag*] [**permanent | track** *object-number*] [**weight** *number*] [**description** *description-text*] [**disabled** | **enabled**] [**global**] command to configure a static route, which is used to specify the network egress after inside destination address translation.

8.3.4 TCP Load Balancing

When the TCP traffic load of an intranet host is excessively heavy, multiple hosts can be deployed to implement TCP service load balancing. In this case, NAT can be used to attain this objective.

Working Principle

Create a virtual host with NAT to provide the TCP service. The virtual host maps to multiple physical hosts. Then the virtual host polls and replaces destination addresses, so as to implement traffic load distribution.

Related Configuration

- **Configuring NAT Interfaces**

- An interface is not an NAT interface by default.
- run the **ip nat { inside | outside }** command to specify a pair of NAT interfaces.
- NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured.

- **Configuring the Address Pool**

- No address pool is configured by default.
- Use the **ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* } command to configure an IP address pool for NAT.

- **Configuring the ACL**

- No ACL is configured by default.
- Use the **access-list** *access-list-number* **permit** *ip-address wildcard* command to configure a destination-based ACL. Note that the ACL must be configured as an extended ACL based on destination IP address matching.

- **Configuring Inside Destination Address Translation**

- Inside destination address translation is not configured by default.
- Use the **ip nat inside destination list** *access-list-number* **pool** *address-pool* [**description** *description-text*] command to configure inside destination address translation. This configuration takes effect on TCP traffic only but not on other traffic, unless additional NAT configuration has been performed.

8.3.5 Constructing a Local Server

A user has deployed three servers (an FTP server, a Web server, and an Email server) in an intranet, and hopes that network hosts in a WAN can access the three servers while common users of the intranet can set the gateway as a device to provide Internet access.

Working Principle

Map one or more internal hosts to a network server, so that users on the WAN obtain corresponding services from the network server.

Related Configuration

- **Configuring NAT Interfaces**

- An interface is not an NAT interface by default.
- run the **ip nat { inside | outside }** command to specify a pair of NAT interfaces.

- NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured.

Configuring Inside Address and Port Translation

- Inside address and port translation is not configured by default.
- Use the **ip nat inside source static** { **udp** | **tcp** } **local-address port global-address port** [**permit-inside**] [**description** *description-text*] command to translate specific inside addresses and ports, so that corresponding services are provided on dedicated ports. For example, TCP port 20 or 21 can be used to construct an FTP server, or TCP port 80 to construct a Web server.
- When there are more than one local server with successive port numbers, use the **ip nat inside source static** { **udp** | **tcp** } **local-address {port-range} port1 port2 global-address {port-range} port3 port4** [**permit-inside**] [**description** *description-text*] command to translate specific inside addresses and ports, so that corresponding services are provided on dedicated ports. For example, TCP port 20 or 21 can be used to construct an FTP server.

8.3.6 ALG

Common NAT can translate the IP address and port in the header of a UDP or TCP packet, but is helpless before fields in application layer data payloads. In many application layer protocols such as multimedia protocols (H.323 and the like), FTP, and SQLNET, the TCP/UDP payload carries address or port information. If such address or port information cannot be translated by NAT, problems may occur.

Working Principle

The ALG technology can parse application layer packet information and perform address translation for multi-channel protocols, so as to translate or process the IP addresses or ports requiring address translation or some fields requiring special processing, thereby guaranteeing the correctness of application layer communications. All types of ALGs are enabled for NAT by default. Currently the protocols that support ALG include DNS, FTP, H323, PPTP, TFTP, RTSP, and SIP.

Related Configuration

Enabling or Disabling ALG

- Use the **no ip nat translation dns** command to disable DNS ALG.
- Use the **no ip nat translation ftp** command to disable FTP ALG.
- Use the **no ip nat translation h323** command to disable H323 ALG.
- Use the **no ip nat translation pptp** command to disable PPTP ALG.
- Use the **no ip nat translation tftp** command to disable TFTP ALG.
- Use the **no ip nat translation rtsp** command to disable RTSP ALG.
- Use the **no ip nat translation sip** command to disable SIP ALG.

8.4 Configuration

Configuration	Description and Command
Configuring Basic NAT	Mandatory configuration. It is used to configure one-to-one NAT for internal PCs to connect to a WAN.

	ip nat inside	Marks the interface as connected to the inside.
	ip nat outside	Marks the interface as connected to the outside.
	Optional configuration. It is used to configure static NAT.	
	ip nat inside source static *local-address global-address* [**permit-inside**] [**netmask** *mask*] [**match** interface] [**description** *description-text*]	Defines the static inside source address translation relationship.
	Optional configuration. It is used to configure dynamic NAT.	
	ip nat pool address-pool start-address end-address { **netmask** mask | **prefix-length** prefix-length } or **ip nat pool** *pool-name* { **netmask** *netmask* | **prefix-length** *prefix-length* } [**type rotary**] **address** *start-ip end-ip* [**match interface** *interface*]	Defines a global IP address pool. For NAT, generally multiple IP addresses are defined. The number of address pools to be defined shall depend on the number of intranet users.
	access-list *access-list-number* **permit** *ip-address wildcard*	Defines an ACL, so that only the addresses matching this ACL are translated.
	ip nat inside source list *access-list-number* { [**pool** *address-pool*] | [**interface** *interface-type interface-number*] } **overload** [**description** *description-text*]	Defines the dynamic source address translation relationship. The *overload* parameter may be omitted. It is used only to keep compatibility with mainstream vendors' configuration.
Configuring NAPT	Mandatory configuration. It is used to configure NAPT.	
	ip nat inside	Marks the interface as connected to the inside.
	ip nat outside	Marks the interface as connected to the outside.
	Optional configuration. It is used to configure static NAPT.	
	ip nat inside source static { **UDP** *local-address port* | **TCP** *local-address port* } *global-address port* [**permit-inside**] [**description** *description-text*]	Defines the static inside source address translation relationship.
	Optional configuration. It is used to configure dynamic NAPT.	
	ip nat pool *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }	Defines a global IP address pool. For NAPT, generally only one IP address is defined.
	access-list *access-list-number* **permit** *ip-address wildcard*	Defines an ACL, so that only the addresses matching this ACL are translated.
	ip nat inside source list *access-list-number* { [**pool** *address-pool*] | [**interface** *interface-type interface-number*] } **overload** [**description** *description-text*]	Defines the dynamic source address translation relationship. The *overload* parameter may be omitted. It is used only to keep compatibility with mainstream vendors' configuration.
Configuring Overlapping NAT	Mandatory configuration. It is used to enable overlapping networks to communicate using NAT.	

	ip nat inside	Marks the interface as connected to the inside.
	ip nat outside	Marks the interface as connected to the outside.
	ip nat inside source static *local-address global-address*	Configures inside source address translation.
	Optional configuration. It is used to configure static NAT.	
	ip nat outside source static *global-address local-address*	Configures static NAT.
	Optional configuration. It is used to configure dynamic NAT.	
	ip nat pool *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }	Defines a global IP address pool.
	access-list *access-list-number* **permit** *ip-address wildcard*	Defines an ACL, so that only the addresses matching this ACL are translated.
	ip nat outside source list *access-list-number* **pool** *address-pool*	Defines the dynamic source address translation relationship. The *overload* parameter may be omitted. It is used only to keep compatibility with mainstream vendors' configuration.
Configuring TCP Load Balancing	Mandatory configuration. It is used to configure destination address polling and translation.	
	ip nat inside	Marks the interface as connected to inside.
	ip nat outside	Marks the interface as connected to outside.
	ip nat pool *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }	Defines an IP address pool, which includes all physical host addresses.
	access-list *access-list-number* **permit** *ip-address wildcard*	Defines an ACL, which matches the virtual host address only. Ensure that the ACL is an extended ACL based on destination IP address matching.
	ip nat inside destination list *access-list-number* **pool** *address-pool*	Defines the dynamic inside destination address translation relationship.
Configuring ALG	Optional configuration. It is used to configure ALG for relevant protocols.	
	ip nat translation { **dns** [**ttl** *ttl_time*] | **ftp** [**port** *port_num*] | **tftp** | **pptp** | **h323** | **rtsp** | **sip** }	Defines ALG for relevant protocols.
Configuring Special NAT Applications	Optional configuration. It is used to configure special NAT applications.	
	ip nat application source list *list-num* **destination** *dest-ip* { **dest-change** *ip-addr* | **src-change** *ip-addr* }	Defines rules for special NAT applications.
Configuring the Interval at Which NAT Sends Gratuitous	Optional configuration. It is used to configure the interval at which gratuitous ARP packets are sent from the local address of NAT.	

ARP Packets	**ip nat keepalive** [*keealive_out*]	Defines the interval at which gratuitous ARP packets are sent from the local address of NAT.

8.4.1 Configuring Basic NAT

Networking Requirements

NAT configuration is required for an intranet to communicate with an extranet by translating an inside private IP address into a globally unique IP address. You can configure static or dynamic NAT or both to implement interconnection and interworking.

Notes

- At least one inside interface and one outside interface need to be configured for basic NAT.
- The newly configured NAT rules take effect on new flows only but not on any existing flows.

Configuration Steps

Configuring the NAT Inside Interface

- Mandatory configuration.
- Configure the LAN interface to connect to the intranet as the NAT inside interface unless otherwise stated.

Configuring the NAT Outside Interface

- Mandatory configuration.
- Configure the WAN interface to connect to the extranet as the NAT outside interface unless otherwise stated.

Configuring Static NAT

- Optional configuration.
- Configure static NAT in global configuration mode when a small number of users in the intranet need to access the extranet.

Configuring Dynamic NAT

- Optional configuration.
- Configure dynamic NAT in global configuration mode when a large number of users in the intranet need to access the extranet.

Verification

N/A

Commands

Configuring the NAT Inside Interface and NAT Outside Interface

Command	**ip nat { inside | outside }**
Parameter Description	**inside**: inside interface **outside**: outside interface
Command Mode	Interface configuration mode
Configuration	NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and

Usage	the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured on the router.

Configuring Static NAT

Command	**ip nat inside source static** *local-address global-address* [**permit-inside**] [**netmask** *mask*] [**match** *interface*] [**description** *description-text*]
Parameter Description	*local-address*: inside address *global-address*: outside address **permit-inside**: permits intranet users to access the *local-ip* host using *global-ip*. **netmask** *mask*: network-segment-to-network-segment address **match** *interface*: specifies the egress interface. **description** *description-text*: description.
Command Mode	Global configuration mode
Configuration Usage	-

Configuring the Address Pool

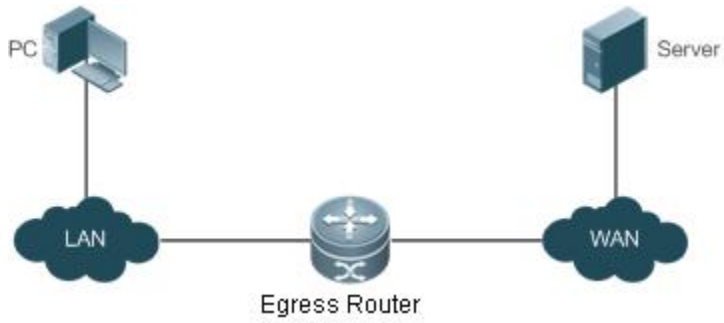
Command	**ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }
Parameter Description	*address-pool*: name of the address pool *start-address*: start IP address *end-address*: end IP address **netmask** *mask*: network mask of the addresses **prefix-length** *prefix-length*: length of the network mask of the addresses
Command Mode	Global configuration mode
Configuration Usage	-

Configuring Dynamic NAT

Command	**ip nat inside source list** *access-list-number* **pool** *address-pool*
Parameter Description	*access-list-number*: ACL number **pool** *address-pool*: name of the address pool
Command Mode	Global configuration mode
Configuration Usage	

Configuration Example

Enabling Intranet Users to Access an Extranet Server

Scenario **Figure 7-5**	
Configuration Steps	Configure **ip nat inside** on the inside interface. Configure **ip nat outside** on the outside interface. Configure a dynamic NAT rule.
A	A# configure terminal A(config)# interface GigabitEthernet 0/0 A(config-if-GigabitEthernet 0/0)# ip address 192.168.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/0)# ip nat inside A(config-if-GigabitEthernet 0/0)# exit A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 200.168.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# ip nat outside A(config-if-GigabitEthernet 0/1)# exit A(config)# ip nat pool net200 200.168.12.2 200.168.12.100 netmask 255.255.255.0 A(config)# ip nat inside source list 1 pool net200 A(config)# access-list 1 permit 192.168.12.0 0.0.0.255
Verification	Use the **show** command to display the configuration.
A	FS# show ip nat translations Pro Inside global Inside local Outside local Outside global tcp 200.168.12.200:2063 192.168.12.65:2063 168.168.12.1:23 168.168.12.1:23

Common Errors

- The inside or outside interface is not configured.
- The ACL configuration is incorrect.

8.4.2 Configuring NAPT

Networking Requirements

In general, traditional NAT is one-to-one address mapping, which, however, cannot meet the requirements of all hosts in intranets to communicate with extranets. For example, when the intranet is in short of global IP addresses or even does not apply for global IP addresses but has only one global IP address to connect to an Internet Service Provider (ISP) while a large number of hosts in the intranet need to access the Internet, NAPT is required in this scenario.

Multiple inside local addresses can map to one inside global address using NAPT.

Notes

- At least one inside interface and one outside interface need to be configured for NAPT.
- The newly configured NAT rules take effect on new flows only but not on any existing flows.

Configuration Steps

Configuring the NAT Inside Interface

- Mandatory configuration.
- Configure the LAN interface to connect to the intranet as the NAT inside interface unless otherwise stated.

Configuring the NAT Outside Interface

- Mandatory configuration.
- Configure the WAN interface to connect to the extranet as the NAT outside interface unless otherwise stated.

Configuring Static NAPT

- Optional configuration.
- Configure static NAPT in global configuration mode when a small number of users in the intranet need to access the extranet.

Configuring Dynamic NAPT

- Optional configuration.
- Configure dynamic NAPT in global configuration mode when a large number of users in the intranet need to access the extranet.

Verification

N/A

Commands

Configuring the NAT Inside Interface and NAT Outside Interface

Command	**ip nat { inside | outside }**
Parameter Description	**inside**: inside interface **outside**: outside interface
Command Mode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured on the router.

Configuring Static NAPT

Command	**ip nat inside source static** { **udp** *local-address port* | **tcp** *local-address port* } *global-address port* [**permit-inside**] [**description** *description-text*]
Parameter	**udp**: UDP

Description	**tcp**: TCP *local-address*: inside local address *port*: inside local port *global-address*: outside global address *port*: outside global port **permit-inside**: permits intranet users to access the *local-ip* host using *global-ip*. **description** *description-text*: Description
Command Mode	Global configuration mode
Configuration Usage	This command is used to build an internal server that external public networks can access. Internal hosts are not allowed to access the internal server using the *global-address* unless **permit-inside** has been configured. If **permit-inside** is not configured, internal hosts can access the internal server by using the *local-address* only.

Configuring the Address Pool

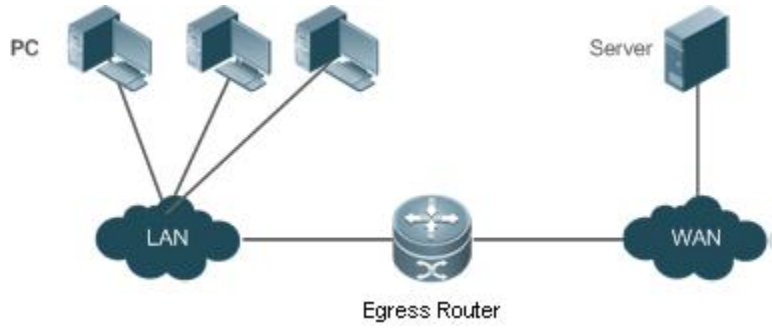
Command	**ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }
Parameter Description	*address-pool*: name of the address pool *start-address*: start IP address *end-address*: end IP address **netmask** *mask*: network mask of the addresses **prefix-length** *prefix-length*: length of the network mask of the addresses
Command Mode	Global configuration mode
Configuration Usage	-

Configuring Dynamic NAPT

Command	**ip nat inside source list** *access-list-number* { [**pool** *address-pool*] | [**interface** *interface-type interface-number*] } **overload** [**description** *description-text*]
Parameter Description	*access-list-number*: ACL number **pool** *address-pool*: name of the address pool **interface** *interface-type interface-number*: implements NAPT using the global address of the outside interface. **overload**: Indicates that each global address in the address pool can be reused for NAPT. Currently, the global addresses are reused even if this parameter is not configured. Therefore, this parameter is used only to keep compatibility with Cisco commands. **description** *description-text*: Description
Command Mode	Global configuration mode
Configuration Usage	-

Configuration Example

Enabling Intranet User to Access an Extranet Server Through NAPT

Scenario **Figure 7-6**	
Configuration Steps	Configure **ip nat inside** on the inside interface. Configure **ip nat outside** on the outside interface. Configure a dynamic NAPT rule.
A	A# configure terminal A(config)# interface GigabitEthernet 0/0 A(config-if-GigabitEthernet 0/0)# ip address 192.168.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/0)# ip nat inside A(config-if-GigabitEthernet 0/0)# exit A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 200.198.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# ip nat outside A(config-if-GigabitEthernet 0/1)# exit A(config)# ip nat pool net200 200.168.12.1 200.168.12.1 netmask 255.255.255.0 A(config)# ip nat inside source list 1 pool net200 A(config)# access-list 1 permit 192.168.12.0 0.0.0.255 A(config)# ip nat inside source static tcp 192.168.12.3 80 200.198.12.1 80
Verification	Use the **show** command to display the configuration.
A	FS# show ip nat translations Pro Inside global Inside local Outside local Outside global tcp 200.168.12.200:2063 192.168.12.65:2063 168.168.12.1:23 168.168.12.1:23 icmp 200.168.12.200:2064 192.168.12.66:2063 168.168.12.1:23 168.168.12.1:23 udp 200.168.12.200:2065 192.168.12.67:2063 168.168.12.1:23 168.168.12.1:23 tcp 200.168.12.200:2066 192.168.12.68:2063 168.168.12.1:23 168.168.12.1:23 tcp 200.168.12.200:2067 192.168.12.69:2063 168.168.12.1:23 168.168.12.1:23

-

Common Errors

- The inside or outside interface is not configured.
- The ACL configuration is incorrect.

8.4.3 Configuring Overlapping NAT

Networking Requirements

When the same IP address is allocated to two private networks to interconnect with each other or the same global IP address is allocated to a private network and a public network, this situation is called address overlapping. Two overlapping network hosts cannot communicate, because both hosts consider that the peer host is in the local network. Overlapping NAT is especially designed to implement the communications between two networks with the same IP address. After overlapping NAT is configured, an extranet host address will be represented as another host address in the intranet, and vice versa.

Notes

- Internal source address translation must be configured before overlapping NAT is configured.
- The newly configured NAT rules take effect on new flows only but not on any existing flows.

Configuration Steps

Configuring the NAT Inside Interface

- Mandatory configuration.
- Configure the LAN interface to connect to the intranet as the NAT inside interface unless otherwise stated.

Configuring the NAT Outside Interface

- Mandatory configuration.
- Configure the WAN interface to connect to the extranet as the NAT outside interface unless otherwise stated.

Configuring Static Translation of Outside Source Address

- Optional configuration.
- Configure static translation of outside source address in global configuration mode when a small number of users in the extranet need to access the intranet.

Configuring Dynamic Translation of Outside Source Address

- Optional configuration.
- Configure dynamic translation of outside source address in global configuration mode when a large number of users in the extranet need to access the intranet.

Configuring an ACL

- ACL configuration is mandatory when dynamic source address mapping is used.
- Restrict the range of users requiring source address translation in the intranet.

Configuring a Static Route

- Mandatory configuration.
- Specify the network egress after inside destination address translation.

Verification

N/A

Commands

Configuring the NAT Inside Interface and NAT Outside Interface

Command	**ip nat { inside | outside }**
Parameter Description	**inside**: inside interface **outside**: outside interface
Command Mode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured on the router.

Configuring Static Translation of Outside Source Address

Command	**ip nat outside source static** *global-address local-address*
Parameter Description	*global-address*: outside global address *local-address*: inside local address
Command Mode	Global configuration mode
Configuration Usage	

Configuring Static Translation of Outside Source Address and Port

Command	**ip nat outside source static** { **tcp** *global-address global-port* | **udp** *global-address global-port* } *local-address local-port*
Parameter Description	*protocol*: protocol number *global-address*: outside global address *global-port*: outside global port *local-address*: inside local address *local-port*: inside local port
Command Mode	Global configuration mode
Configuration Usage	-

Configuring the Address Pool

Command	**ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }
Parameter Description	*address-pool*: name of the address pool *start-address*: start IP address *end-address*: end IP address **netmask** *mask*: network mask of the addresses **prefix-length** *prefix-length*: length of the network mask of the addresses
Command Mode	Global configuration mode

Configuration Usage	--

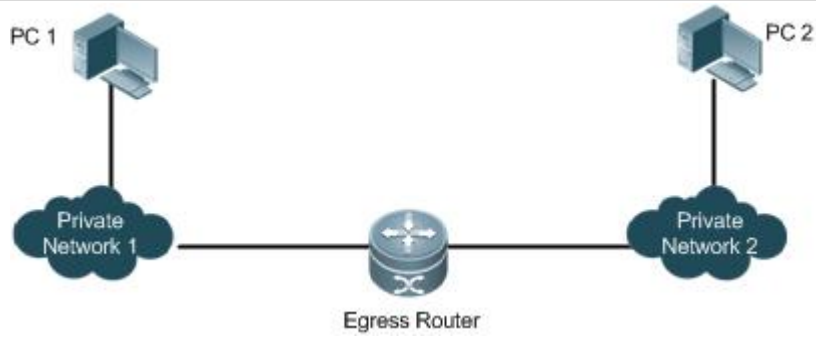
Configuring Dynamic Translation of Outside Source Address

Command	**ip nat outside source list** *access-list-number* **pool** *pool-name*
Parameter Description	*access-list-number*: ACL number **pool** *pool-name*: name of the address pool
Command Mode	Global configuration mode
Configuration Usage	

Configuration Example

The following configuration example describes configuration related to static translation of outside source address.

Static Translation of Outside Source Address

Scenario **Figure 7-7**	
Configuration Steps	Configure **ip nat inside** on the inside interface. Configure **ip nat outside** on the outside interface. Configure a rule for dynamic translation of inside source address. Configure a rule for static translation of outside source address.
A	A# configure terminal A(config)# interface GigabitEthernet 0/0 A(config-if-GigabitEthernet 0/0)# ip address 192.168.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/0)# ip nat inside A(config-if-GigabitEthernet 0/0)# exit A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 200.198.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# ip nat outside A(config-if-GigabitEthernet 0/1)# exit A(config)# ip nat pool net200 200.168.12.2 200.168.12.100 netmask 255.255.255.0 A(config)# ip nat inside source list 1 pool net200 A(config)# access-list 1 permit 192.168.12.0 0.0.0.255 A(config)# ip nat outside source static 192.168.12.3 172.16.10.1

	A(config)# ip route 172.16.10.0 255.255.255.0 200.198.12.2
Verification	Use the **show** command to display the configuration.
A	FS# show ip nat translations Pro Inside global Inside local Outside local Outside global tcp 200.168.12.200:2063 192.168.12.65:2063 172.16.10.1:23 168.168.12.3:23

Common Errors

- The inside or outside interface is not configured.
- The ACL configuration is incorrect.
- No static route is configured or no IP address is configured for the outside interface, so that the router does not know to which interface a data packet should be sent after NAT or from which interface a data packet is received after NAT.

8.4.4 Configuring TCP Load Balancing

Networking Requirements

When the TCP traffic load of an intranet host is excessively heavy, multiple hosts can be deployed to implement TCP service load balancing. In this case, NAT can be used to attain this objective. In the following configuration, a virtual host address is defined, so that all TCP connections from extranets to the virtual host are distributed by a router to multiple physical hosts, so as to implement traffic load balancing.

Notes

The newly configured NAT rules take effect on new flows only but not on any existing flows.

Configuration Steps

Configuring the NAT Inside Interface

- Mandatory configuration.
- Configure the LAN interface to connect to the intranet as the NAT inside interface unless otherwise stated.

Configuring the NAT Outside Interface

- Mandatory configuration.
- Configure the WAN interface to connect to the extranet as the NAT outside interface unless otherwise stated.

Configuring Dynamic Translation of Inside Destination Address

- Mandatory configuration.
- Configure dynamic translation of inside destination address in global configuration mode for TCP load balancing.

Verification

N/A

Commands

Configuring the NAT Inside Interface and NAT Outside Interface

Command	**ip nat { inside | outside }**
Parameter Description	**inside**: inside interface **outside**: outside interface
Command Mode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured on the router.

Configuring the Address Pool

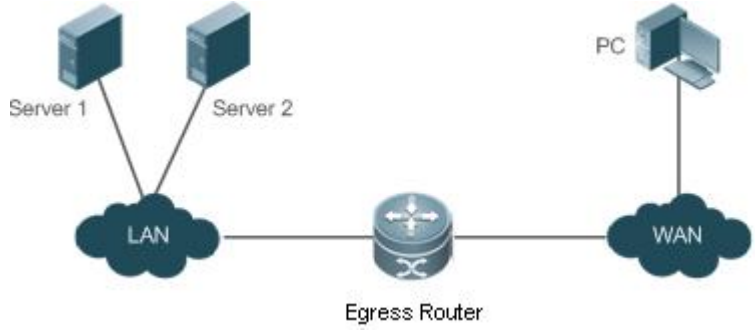
Command	**ip nat pool** *pool-name start-ip end-ip* { **netmask** *netmask* | **prefix-length** *prefix-length* } [**type rotary**]
Parameter Description	*address-pool*: name of the address pool *start-address*: start IP address *end-address*: end IP address **netmask** *mask*: network mask of the addresses **prefix-length** *prefix-length*: length of the network mask of the addresses **type rotary**: NAT address pool type. Rotary type guarantees equal chance of every address to be assigned. Whether **type rotary** is configured or not, the NAT address pool type is rotary. This parameter is introduced for compatibility with Cisco.
Command Mode	Global configuration mode
Configuration Usage	

Configuring Dynamic Translation of Inside Destination Address

Command	**ip nat inside destination list** *access-list-number* **pool** *address-pool* [**description** *description-text*]
Parameter Description	*access-list-number*: ACL number **pool** *pool-name*: name of the address pool **description** *description-text*: Description
Command Mode	Global configuration mode
Configuration Usage	

Configuration Example

Enabling Extranet User to Access an Intranet Server

Scenario **Figure 7-8**	

Configuration Steps	Configure **ip nat inside** on the inside interface. Configure **ip nat outside** on the outside interface. Configure a rule for dynamic inside destination address translation.
A	A# configure terminal A(config)# interface GigabitEthernet 0/0 A(config-if-GigabitEthernet 0/0)# ip address 10.10.10.1 255.255.255.0 A(config-if-GigabitEthernet 0/0)# ip nat inside A(config-if-GigabitEthernet 0/0)# exit A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 200.198.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# ip nat outside A(config-if-GigabitEthernet 0/1)# exit A(config)# ip nat pool realhosts 10.10.10.2 10.10.10.3 netmask 255.255.255.0 type rotary A(config)# ip nat inside destination list 100 pool realhosts A(config)# access-list 100 permit ip any host 10.10.10.100
Verification	Use the **show** command to display the configuration.
A	FS# show ip nat translations Pro Inside global Inside local Outside local Outside global tcp 10.10.10.100:23 10.10.10.2:23 100.100.100.100:1178 100.100.100.100:1178 tcp 10.10.10.100:23 10.10.10.3:23 200.200.200.200:1024 200.200.200.200:1024

Common Errors

- The inside or outside interface is not configured.
- The ACL configuration is incorrect. Note that the ACL must be configured as an extended ACL based on destination IP address matching.
- The above configuration takes effect on TCP traffic only but not on other traffic, unless additional NAT configuration has been performed.

8.4.5 Configuring ALG

Networking Requirements

In general, NAT translates only IP address and port information in the header of a packet but does not analyze fields in the application layer data payload of the packet. However, for some special protocols, such as FTP, DNS, and FTFP, the data payloads of their packets may contain IP address or port information. If such information is not translated by NAT, certain problems may occur. The NAT ALG technology can parse application layer packet information and perform address translation for multi-channel protocols, so as to translate or process the IP addresses or ports requiring address translation or some fields requiring special processing, thereby guaranteeing the correctness of application layer communications.

Notes

- At least one inside interface and one outside interface need to be configured during the configuration of ALG.
- The newly configured NAT rules take effect on new flows only but not on any existing flows.

Configuration Steps

Configuring the NAT Inside Interface

- Mandatory configuration.
- Configure the LAN interface to connect to the intranet as the NAT inside interface unless otherwise stated.

Configuring the NAT Outside Interface

- Mandatory configuration.
- Configure the WAN interface to connect to the extranet as the NAT outside interface unless otherwise stated.

Configuring Static NAT

- Optional configuration.
- Configure static NAT in global configuration mode when a small number of users in the intranet need to access the extranet.

Configuring Dynamic NAT

- Optional configuration.
- Configure dynamic NAT in global configuration mode when a large number of users in the intranet need to access the extranet.

Configuring ALG

- Optional configuration.
- The ALG configuration is mandatory if the DNS, FTP, TFTP, PPTP, H323, RTSP, or SIP protocol in the environment needs to implement NAT transversal for communications.

Verification

N/A

Commands

Configuring the NAT Inside Interface and NAT Outside Interface

Command	**ip nat { inside | outside }**
Parameter Description	**inside**: inside interface **outside**: outside interface
Command Mode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured on the router.

Configuring Static NAT

Command	**ip nat inside source static** *local-address global-address* [**permit-inside**] [**netmask** *mask*] [**match** *interface*] [**description**

	description-text]
Parameter Description	*local-address*: inside address *global-address*: outside address **permit-inside**: permits intranet users to access the *local-ip* host using *global-ip*. **netmask** *mask*: network-segment-to-network-segment address **match** *interface*: specifies the egress interface. **description** *description-text*: Description
Command Mode	Global configuration mode
Configuration Usage	-

Configuring the Address Pool

Command	**ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }
Parameter Description	*address-pool*: name of the address pool *start-address*: start IP address *end-address*: end IP address **netmask** *mask*: network mask of the addresses **prefix-length** *prefix-length*: length of the network mask of the addresses
Command Mode	Global configuration mode
Configuration Usage	

Configuring Dynamic NAT

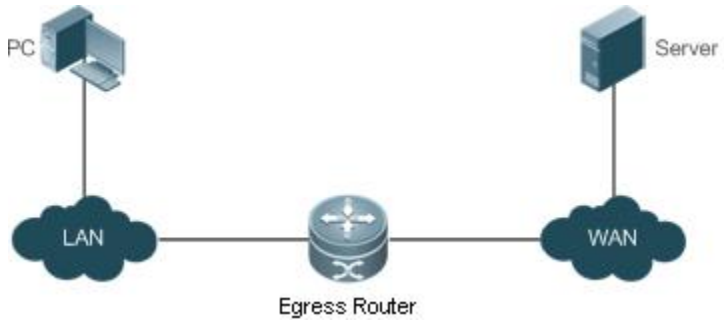
Command	**ip nat inside source list** *access-list-number* **pool** *address-pool* [**description** *description-text*]
Parameter Description	*access-list-number*: ACL number **pool** *address-pool*: name of the address pool **description** *description-text*: Description
Command Mode	Global configuration mode
Configuration Usage	

Configuring ALG

Command	**ip nat translation** { **dns** [**ttl** *ttl_time*] | **ftp** [**port** *port_num*] | **tftp** | **pptp** | **h323** | **rtsp** | **sip** }
Parameter Description	**ttl**: defines the NAT timeout interval of the UDP connection of the DNS application. The default value is 0. *port_num*: defines the port number used for the FTP application. The default value is 21.
Command Mode	Global configuration mode
Configuration Usage	

Configuration Example

Enabling Intranet Users to Access an Extranet Server

Scenario **Figure 7-9**	
Configuration Steps	Configure **ip nat inside** on the inside interface. Configure **ip nat outside** on the outside interface. Configure a dynamic NAT rule. Configure ALG.
A	A# configure terminal A(config)# interface GigabitEthernet 0/0 A(config-if-GigabitEthernet 0/0)# ip address 192.168.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/0)# ip nat inside A(config-if-GigabitEthernet 0/0)# exit A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 200.168.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# ip nat outside A(config-if-GigabitEthernet 0/1)# exit A(config)# ip nat pool net200 200.168.12.2 200.168.12.100 netmask 255.255.255.0 A(config)# ip nat inside source list 1 pool net200 A(config)# access-list 1 permit 192.168.12.0 0.0.0.255 A(config)# ip nat translation ftp 23
Verification	Use the **show** command to display the configuration.
A	FS# show ip nat translations Pro Inside global Inside local Outside local Outside global tcp 200.168.12.200:2063 192.168.12.65:2063 168.168.12.1:23 168.168.12.1:23

Common Errors

- The inside or outside interface is not configured.
- The ACL configuration is incorrect.

8.4.6 Configuring Special NAT Applications

Networking Requirements

For some advanced applications of NAT, the source addresses or destination addresses of some specific IP packets need to be modified.

Notes

- At least one inside interface and one outside interface need to be configured for special NAT applications.
- The newly configured NAT rules take effect on new flows only but not on any existing flows.

Configuration Steps

Configuring the NAT Inside Interface

- Mandatory configuration.
- Configure the LAN interface to connect to the intranet as the NAT inside interface unless otherwise stated.

Configuring the NAT Outside Interface

- Mandatory configuration.
- Configure the WAN interface to connect to the extranet as the NAT outside interface unless otherwise stated.

Configuring Static NAT

- Optional configuration.
- Configure static NAT in global configuration mode when a small number of users in the intranet need to access the extranet.

Configuring Dynamic NAT

- Optional configuration.
- Configure dynamic NAT in global configuration mode when a large number of users in the intranet need to access the extranet.

Configuring Special NAT Applications

- Optional configuration.
- This configuration is mandatory if special address translation is required for the communications of some applications.

Verification

N/A

Commands

Configuring the NAT Inside Interface and NAT Outside Interface

Command	**ip nat { inside | outside }**
Parameter Description	**inside**: inside interface **outside**: outside interface
Command Mode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured on the router.

Configuring Static NAT

Command	**ip nat inside source static** *local-address global-address* [**permit-inside**] [**netmask** *mask*] [**match** *interface*] [**description** *description-text*]
Parameter Description	*local-address*: inside address *global-address*: outside address **permit-inside**: permits intranet users to access the *local-ip* host using *global-ip*. **netmask** *mask*: network-segment-to-network-segment address **match** *interface*: specifies the egress interface. **description** *description-text*: Description
Command Mode	Global configuration mode
Configuration Usage	-

Configuring the Address Pool

Command	**ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }
Parameter Description	*address-pool*: name of the address pool *start-address*: start IP address *end-address*: end IP address **netmask** *mask*: network mask of the addresses **prefix-length** *prefix-length*: length of the network mask of the addresses
Command Mode	Global configuration mode
Configuration Usage	

Configuring Dynamic NAT

Command	**ip nat inside source list** *access-list-number* **pool** *address-pool*
Parameter Description	*access-list-number*: ACL number **pool** *address-pool*: name of the address pool
Command Mode	Global configuration mode
Configuration Usage	

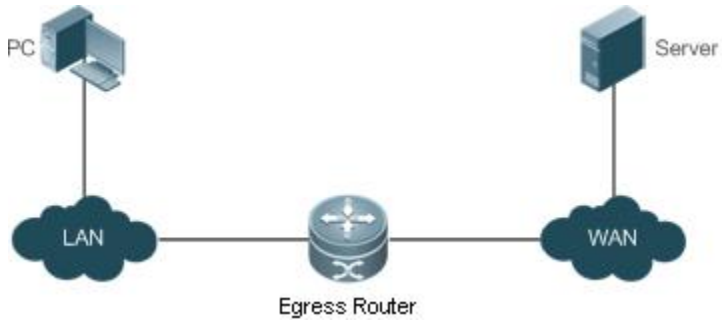
Configuring Special NAT Applications

Command	**ip nat application source list** *list-num* **destination** *dest-ip* { **dest-change** *ip-addr* | **src-change** *ip-addr* }
Parameter Description	*local-address*: inside address *global-address*: outside address **permit-inside**: permits intranet users to access the *local-ip* host using *global-ip*. **netmask** *mask*: network-segment-to-network-segment address **match** *interface*: specifies the egress interface.
Command Mode	Global configuration mode
Configuration	

Usage	

Configuration Example

Implementing the DNS Relay Service

Scenario Figure 7-10	
Configuration Steps	Configure **ip nat inside** on the inside interface. Configure **ip nat outside** on the outside interface. Configure a dynamic NAT rule. Configure special NAT applications.
A	A#configure terminal A(config)# interface GigabitEthernet 0/0 A(config-if-GigabitEthernet 0/0)# ip address 192.168.1.1 255.255.255.0 A(config-if-GigabitEthernet 0/0)# ip nat inside A(config-if-GigabitEthernet 0/0)# exit A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 200.168.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# ip nat outside A(config-if-GigabitEthernet 0/1.)# exit A(config)# ip nat pool net200 200.168.12.2 200.168.12.10 netmask 255.255.255.0 A(config)# ip nat inside source list 1 pool net200 A(config)# access-list 1 permit 192.168.12.0 0.0.0.255 A(config)# ip nat application source list 1 destination udp 192.168.1.1 53 dest-change 202.101.98.55 53 A(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Verification	

Common Errors

- The inside or outside interface is not configured.

8.4.7 Configuring the Interval at Which NAT Sends Gratuitous ARP Packets

Networking Requirements

Configure the interval at which gratuitous ARP packets are sent from addresses in the NAT address pool, so as to avoid address conflicts.

Notes

- Sending gratuitous ARP packets is disabled by default on the NAT device.
- Gratuitous ARP packets are sent to the outside interface only.

Configuration Steps

Configuring the NAT Inside Interface

- Mandatory configuration.
- Configure the LAN interface to connect to the intranet as the NAT inside interface unless otherwise stated.

Configuring the NAT Outside Interface

- Mandatory configuration.
- Configure the WAN interface to connect to the extranet as the NAT outside interface unless otherwise stated.

Configuring Static NAT

- Optional configuration.
- Configure static NAT in global configuration mode when a small number of users in the intranet need to access the extranet.

Configuring Dynamic NAT

- Optional configuration.
- Configure dynamic NAT in global configuration mode when a large number of users in the intranet need to access the extranet.

Configuring the Interval at Which NAT Sends Gratuitous ARP Packets

- Optional configuration.
- NAT needs to consider some addresses matching the configured rule as local addresses. This configuration is performed to avoid address conflicts.

Verification

N/A

Commands

Configuring the NAT Inside Interface and NAT Outside Interface

Command	**ip nat { inside | outside }**
Parameter Description	**inside**: inside interface **outside**: outside interface
Command Mode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured on the router.

Configuring Static NAT

Command	**ip nat inside source static** *local-address global-address* [**permit-inside**] [**netmask** *mask*] [**match** *interface*] [**description** *description-text*]
Parameter Description	*local-address*: inside address *global-address*: outside address **permit-inside**: permits intranet users to access the *local-ip* host using *global-ip*. **netmask** *mask*: network-segment-to-network-segment address **match** *interface*: specifies the egress interface. **description** *description-text*: Description
Command Mode	Global configuration mode
Configuration Usage	

Configuring the Address Pool

Command	**ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }
Parameter Description	*address-pool*: name of the address pool *start-address*: start IP address *end-address*: end IP address **netmask** *mask*: network mask of the addresses **prefix-length** *prefix-length*: length of the network mask of the addresses
Command Mode	Global configuration mode
Configuration Usage	-

Configuring Dynamic NAT

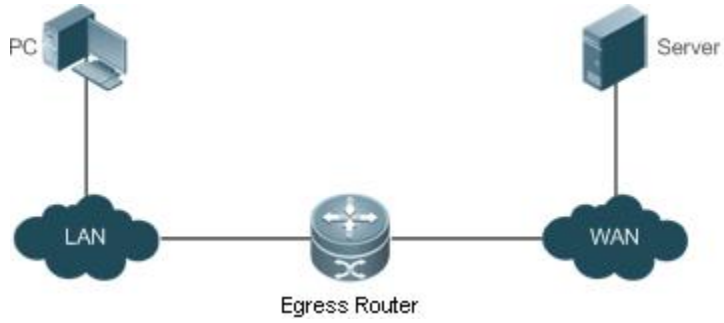
Command	**ip nat inside source list** *access-list-number* **pool** *address-pool* [**description** *description-text*]
Parameter Description	*access-list-number*: ACL number **pool** *address-pool*: name of the address pool **description** *description-text*: Description
Command Mode	Global configuration mode
Configuration Usage	-

Configuring the Interval at Which NAT Sends Gratuitous ARP Packets

Command	**ip nat keepalive** [*keealive_out*]
Parameter Description	*keealive_out*: the interval at which gratuitous ARP packets are sent from the local address of NAT.
Command Mode	Global configuration mode
Configuration Usage	-

Configuration Example

Implementing the Sending of Gratuitous ARP Packets regularly

Scenario Figure 7-11	
Configuration Steps	Configure **ip nat inside** on the inside interface. Configure **ip nat outside** on the outside interface. Configure a dynamic NAT rule. Configure the periodical sending of gratuitous ARP packets.
A	A#configure terminal A(config)# interface GigabitEthernet 0/0 A(config-if-GigabitEthernet 0/0)# ip address 192.168.1.1 255.255.255.0 A(config-if-GigabitEthernet 0/0)# ip nat inside A(config-if-GigabitEthernet 0/0)# exit A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 200.168.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# ip nat outside A(config-if-GigabitEthernet 0/1.)# exit A(config)# ip nat pool net200 200.168.12.2 200.168.12.10 netmask 255.255.255.0 A(config)# ip nat inside source list 1 pool net200 A(config)# access-list 1 permit 192.168.12.0 0.0.0.255 A(config)# ip nat keepalive 10
Verification	-

Common Errors

- The inside or outside interface is not configured.
- NAT rule is not correct.

8.5 Monitoring

Displaying

Function	Command
Displays NAT records.	**show ip nat translations** [*acl_num*] [**icmp** | **tcp** | **udp**] [**verbose**]

9 Configuring MLLB

9.1 Overview

Multi Link load balance (MLLB) is a solution to load balancing between multiple links.

FS gateways can implement MLLB, resolving load balancing problems, freeing users of configuration of a great number of static routes, and enabling users to access external networks over multiple links.

With MLLB of FS gateways, traffic can be properly distributed, according to a policy, to multiple links applying equal cost multipath routing (ECMP), which improves the utilization rate of the links.

MLLB is implemented based on link bandwidth or link load.

MLLB is applicable to load balancing services applying ECMP of a same carrier on a network with multiple egress interfaces.

9.2 Applications

Application	Description
Balancing Load Based on Bandwidth Through Multiple Egress Interfaces on Campus Network	One or more Internet service providers (ISPs) provide multilink network services.

9.2.1 Balancing Load Based on Bandwidth Through Multiple Egress Interfaces on Campus Network

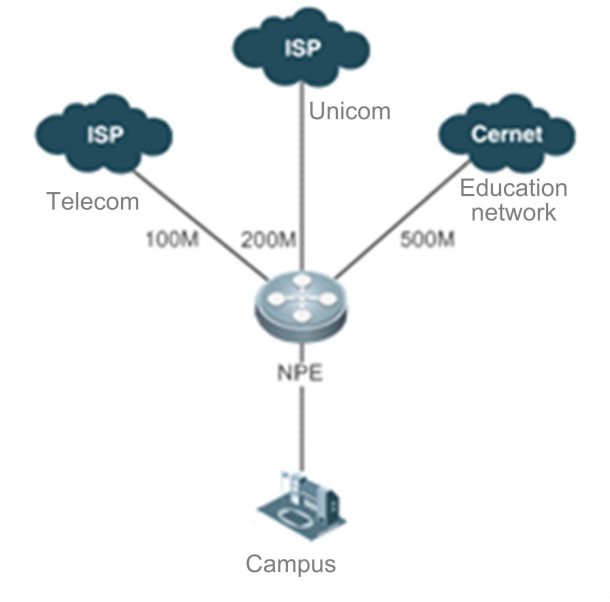
Scenario

Multiple ISPs provide multilink network services.

As shown in Figure 8-1, China Telecom, China Unicom, and CERNET provide the egress network services for campus network users.

- Campus users access external networks, forming ECMP.
- Load is balanced based on bandwidth.

Figure 9-1



Deployment

- Enable MLLB.
- Configure a bandwidth-based load balancing policy.
- Prioritize egress interfaces.

9.3 Features

Basic Concepts

Flow

Flows or flow sessions are packets with the same 5-tuple (source and destination IP addresses, source and destination ports, and protocol ID) within a period of time.

ECMP

ECMP enables one or more egress interfaces or next hops if a routing prefix is given.

Link Bandwidth

Link bandwidth is an indicator measuring available resources of a link. Unlike the transmission rate of a physical interface with the upper limit specified by the operator, link bandwidth generally refers to the downlink bandwidth.

Link Load

Link load indicates the utilization rate of a link, which can be calculated by dividing the packet receiving rate of a physical interface by link bandwidth.

Threshold

A threshold, also referred to as a load threshold, indicates the alarm line of the bandwidth utilization rate of an egress interface. If the egress traffic exceeds the threshold, MLLB enables corresponding operations.

MLLB is not supported in the VPN dialup scenario. At present, the gateway cannot differentiate parent flows from child flows in the VPN dialup scenario. Consequently, MLLB may forward different packets to different egress interfaces, resulting in VPN negotiation failure.

Overview

Feature	Description
MLLB Switch	Enables or disables MLLB.
Bandwidth-based Load Balancing	Selects an ECMP egress link based on the link bandwidth for load balancing.
Weight Value Definition	Specifies bandwidth weights of an interface.
Load-based Load Balancing	Selects a link with the minimum load based on ECMP link load for load balancing.
Source IP-based Link Selection	Selects a link based on the source IP address to balance load. This function must be used in conjunction with the bandwidth-based policy.
Preferred Links	Selects the preferred link to balance load if all egress links are overloaded.
Load Monitoring	Generally, the downlink traffic of an egress interface is greater than the uplink traffic. For a LAN server, its uplink traffic may be greater than the downlink traffic. In this case, the load monitoring function can be enabled to monitor the uplink traffic. This function must be used in conjunction with the load-based policy.
Load Thresholds	Uses load thresholds as references for adding a link to balance load or removing a link from balancing load. If the load of a link exceeds an upper limit, the link will not be selected for load balancing. If the load of the link becomes smaller than a lower limit, the link is selected to balance load.
Automatic Network Detection	Automatically detects current network.

9.3.1 MLLB Switch

The MLLB switch is used to enable or disable MLLB.

Working Principle

After MLLB is enabled, load balancing is performed for ECMP egress flows according to the default policy (load-based policy).

After MLLB is disabled, load balancing is not performed for ECMP egress flows.

Related Configuration

Enabling MLLB

MLLB of FS gateways is disabled by default.

Run the **mllb enable** command in global configuration mode to enable MLLB.

After MLLB is enabled, load balancing is performed for ECMP egress flows according to the default policy.

Disabling MLLB

MLLB of FS gateways is disabled by default.

Run the **no mllb enable** command in global configuration mode to disable MLLB.

After MLLB is disabled, load balancing is not performed for ECMP egress flows.

9.3.2 Bandwidth-based Load Balancing

According to the bandwidth-based policy, load is balanced based on the uplink or downlink bandwidth of the ECMP egress interface. Traffic of an egress interface varies with the bandwidth of the egress interface.

Working Principle

For a given ECMP egress interface, bandwidth weights of links are calculated. Greater bandwidth indicates a greater weight. Bandwidth is directly proportional to the weight.

If the traffic of an egress interface exceeds a threshold, the egress interface will not be used for routing. If the traffic of all egress interfaces exceeds the threshold, MLLB cannot balance load based on the bandwidth. In this case, users can specify a preferred egress interface for load balancing.

➘ Calculating Bandwidth Weight

Supposed that the total bandwidth of ECMP egress interfaces is S, bandwidth of one egress interface is Bi, base weight is base, and the weight value is Wi, the weight value is calculated according to the following formula:

$Wi = Bi \times base / S$

Related Configuration

➘ Enabling Bandwidth-based Policy of MLLB

MLLB of FS gateway balances load based on bandwidth by default.

Run the **mllb policy bandwidth** command in global configuration mode to enable the bandwidth-based policy.

After the bandwidth-based policy is enabled, MLLB will distribute traffic based on the bandwidth weight.

9.3.3 Weight Value Definition

According to the bandwidth-based policy, load is balanced based on the uplink or downlink bandwidth of the ECMP egress. Bandwidth weights can be defined by users.

Working Principle

Load is balanced according to the uplink or downlink bandwidth by default. To change the bandwidth utilization rate of an interface, define a weight value. For example, if the bandwidth of an interface is 100,000 kbps, set the weight value to 150,000 kbps to increase the bandwidth utilization rate; if the bandwidth of an interface is 100,000 kbps, set the weight value to 50,000 kbps to decrease the bandwidth utilization rate.

Related Configuration

➘ Defining Weight Value

The downlink bandwidth of an interface is used as a weight value by default.

Run the **mllb interface** *interface-name* **weight** *weight-number* command in global configuration mode to change the weight value of an interface.

After the weight value is defined, load of the interface will not be balanced based on the downlink bandwidth anymore, and therefore the downlink bandwidth change of the interface will not be sensed. In this case, load is balanced based on the specified weight value.

9.3.4 Load-based Load Balancing

According to the load-based policy, load is balanced based on the uplink or downlink load of the ECMP egress interface. The link with the minimum load is selected to distribute traffic of new flows.

Working Principle

For a given ECMP egress interface, the uplink or downlink load is obtained, and the link with the minimum load is selected preferentially to distribute traffic.

If the traffic of an egress interface exceeds a threshold, the egress interface will not be used for routing. If the traffic of all egress interfaces exceeds the threshold, MLLB cannot balance load based on load. In this case, users can specify a preferred egress interface to distribute traffic.

Related Configuration

Enabling Load-based Policy of MLLB

Run the **mllb policy load** command in global configuration mode to enable the load-based policy.

After the load-based policy is enabled, MLLB will distribute traffic based on the link load.

9.3.5 Source IP-based Link Selection

MLLB uses the source IP address in combination with the bandwidth-based policy to avoid traffic of flows of the same client to be distributed to different egress links, reducing the risk of network access abnormalities.

Working Principle

For a given ECMP egress interface, traffic is distributed to a link according to the source IP address of flows.

If the traffic of an egress interface does not exceed a threshold, traffic of flows with the same source IP address will be distributed to the same egress link.

If the traffic of an egress interface exceeds a threshold, the egress interface will not be used for routing. If the traffic of all egress interfaces exceeds the threshold, MLLB cannot balance load based on load. In this case, users can specify a preferred egress interface to distribute traffic.

Related Configuration

Enabling Source IP-based Link Selection of MLLB

MLLB of FS gateways balances load based on source and destination IP addresses by default.

Run the **mllb load-sharing original** command in global configuration mode to enable source IP-based link selection of MLLB.

After this function is enabled, MLLB will distribute traffic of ECMP egress flows based on the source IP address, and therefore traffic of flows of the same client will be distributed to the same egress interface.

9.3.6 Preferred Links

MLLB supports preferred link settings. When the egress links of the ECMP are overloaded, traffic of flows will be distributed to the preferred link.

Working Principle

If the egress traffic does not exceed the threshold, traffic is distributed according to the policy of MLLB.

If the egress traffic exceeds the threshold, traffic is distributed to the preferred link.

Related Configuration

Enabling Preferred Link of MLLB

The preferred link function of MLLB of FS gateways is disabled by default.

Run the **mllb first-choice** *interface-type interface-number* command in global configuration mode to enable the preferred link function of MLLB.

Run the **no mllb first-choice** command in global configuration mode to disable the preferred link function of MLLB.

When the egress links of the ECMP are overloaded, traffic will be distributed to the preferred egress if this function is enabled. Otherwise, MLLB cannot balance load.

The preferred link function is supported by the default ECMP route only.

9.3.7 Load Monitoring

MLLB supports load monitoring settings. Both the uplink and downlink load can be monitored.

Working Principle

If the uplink load is monitored, MLLB selects the link with the minimum load to distribute traffic according the uplink load.

If the downlink load is monitored, MLLB selects the link with the minimum load to distribute traffic according the downlink load.

If the traffic of an egress interface exceeds a threshold, the egress interface will not be used for routing. If the traffic of all egress interfaces exceeds the threshold, MLLB cannot balance load based on load. In this case, users can specify a preferred egress interface to distribute traffic.

Related Configuration

Enabling Load Monitoring of MLLB

MLLB of FS gateways monitors the downlink load by default.

Run the **load-monitor uplink** command in global configuration mode to enable uplink load monitoring of MLLB.

Run the **no load-monitor** command in global configuration mode to enable downlink load monitoring of MLLB.

9.3.8 Load Thresholds

MLLB supports load threshold settings. Both upper and lower limits can be configured.

Working Principle

According to the load monitoring result, if the load of a link exceeds the upper limit, the link is configured with overload flag and will not balance load.

According to the load monitoring result, if the load of a link is smaller than the lower limit and the link has been configured with the overload flag, the link flag will be removed and the link will balance load again.

According to the load monitoring result, if the load of a link stays between the upper limit and lower limit, the link status remains unchanged.

Related Configuration

Configuring Load Thresholds of MLLB

The default upper and lower limits of MLLB of FS gateways are both 100.

Run the **mllb threshold** *percent-upper* / [**lower** *percent-lower*] command in global configuration mode to configure load thresholds of MLLB.

Run the **no threshold** command in global configuration mode to restore the default settings.

9.3.9 Automatic Network Detection

This function can automatically detect the current network.

Working Principle

User experience is subject to delay in resolving a DNS name and reachability of a parsed IP address. The automatic detection function quantifies network experience from two aspects: Obtain traffic delay, half-open connections and traffic volume from a flow table to quantify overall network experience of the current gateway, and record data of a moment to facilitate future queries; detect the accessibility of a mainstream domain name and record DNS resolution result, TCP connections, and HTTP Get delay according to the specified DNS server and egress interface to quantify the stability of the DNS server.

Related Configuration

Enabling Automatic Detection Function

The automatic detection function is disabled by default.

Run the **mllb detect domain enable** and **mllb detect network enable** commands in global configuration mode to enable this function.

Run the **no mllb detect domain enable** and **no mllb detect network enable** commands in global configuration mode to disable this function.

Configuring Domain Name

A domain name must be configured. A maximum of 32 domain names can be configured.

Run the **mllb detect domain add** *domain-name* command in global configuration mode to configure a domain name.

Run the **no mllb detect domain add** *domain-name* command in global configuration mode to delete a domain name.

Configuring DNS Server and Interface

To implement automatic detection, a domain name, DNS server, and interface must be configured. A maximum of 32 DNS servers and interfaces can be configured.

Run the **mllb detect domain dns-server** *dns-ip interface-name* command in global configuration mode to configure a DNS server and an interface.

Run the **mllb detect domain dns-server** *dns-ip interface-name* **source-ip** *source-ip-address* command to specify a source IP address for network detection.

Run the **no mllb detect domain dns-server** *dns-ip interface-name* command in global configuration mode to delete the DNS server and interface.

Configuring Detection Period

The domain name detection period and network detection period are both five minutes by default.

Run the **mllb detect domain interval** *interval-time* command in global configuration mode to configure the domain name detection period.

Run the **mllb detect network interval** *interval-time* command in global configuration mode to configure the network detection period.

Run the **no mllb detect domain interval** command in global configuration mode to restore the default domain name detection period.

Run the **no mllb detect network interval** command in global configuration mode to restore the default network detection.

#endif

9.4 Configuration

Configuration	Description and Command	
Configuring Bandwidth-based Policy of MLLB	(Mandatory) It is used to create bandwidth-based policies to balance load.	
	mllb enable	Enables MLLB.
	mllb policy bandwidth	Enables the bandwidth-based policy of MLLB.
	bandwidth *kilobits*	Configures link bandwidth.
	(Optional) It is used to configure the preferred link and threshold.	
	mllb load-sharing original	Distributes traffic of flows with the same source IP address to the same egress link.
	mllb first-choice *interface-type interface-number*	Configures a L3 interface as a preferred egress interface.
	mllb threshold { *percent-upper* / [**lower** *percent-lower*] }	Sets the load threshold. The value indicates a percentage and ranges from 1 to 100. The **percent-upper** parameter indicates an upper limit, and the **percent-lower** parameter indicates a lower limit.
Configuring Load-based Policy of MLLB	(Mandatory) It is used to create load-based policies to balance load.	
	mllb enable	Configures the link bandwidth.
	mllb policy load	Enables the load-based policy of MLLB.
	(Optional) It is used to configure the preferred link, threshold, and update period.	

	load-monitor uplink	Configures the link monitoring direction (downlink or uplink). The default direction is downlink.
	mllb first-choice *interface-type interface-number*	Configures a L3 interface as a preferred egress interface.
	mllb threshold { *percent-upper* / [**lower** *percent-lower*] }	Sets the load threshold. The value indicates a percentage and ranges from 1 to 100. The **percent-upper** parameter indicates an upper limit, and the **percent-lower** parameter indicates a lower limit.
	mllb load-interval *refresh-time*	Sets the link monitoring period.

9.4.1 Configuring Bandwidth-based Policy of MLLB

Configuration Effect

- Balance load based on bandwidth-based policies to distribute ECMP egress traffic according to bandwidth.

Notes

- MLLB is effective to ECMP egress flows. Therefore, ECMP must be configured on the network.
- To implement traffic distribution based on bandwidth, bandwidth sizes must be configured on gateway interfaces.

Configuration Steps

Enabling MLLB

- Mandatory. Enable MLLB in global configuration mode.

Configuring Bandwidth-based Policy of MLLB

- Mandatory. Configure the bandwidth-based policy in global configuration mode.

Configuring Interface Bandwidth

- Mandatory. Configure interface bandwidth in interface configuration mode according to actual bandwidth.

Defining Weight Value

- Optional. Configure a weight value in global configuration mode according to the actual bandwidth.

Configuring Source IP Address

- Optional. Traffic is distributed based on the source and destination IP addresses by default. The configuration is mandatory if source IP-based link selection is required.
- Configure the source IP address in global configuration mode.

Configuring Preferred Link

- Optional. This function is disabled by default. The configuration is mandatory if the preferred link is required.
- Configure the preferred link in global configuration mode.

Configuring Load Thresholds

- Optional. The default upper and lower limits are both 100. The configuration is mandatory if the load thresholds need to be changed.
- Configure the load thresholds in global configuration mode.

Verification

Verify that traffic of the ECMP egress flows is distributed according to the load-based policy of MLLB.

- Check whether the egress traffic is distributed based on the bandwidth-based policy.
- Check whether traffic is distributed to the preferred link if all ECMP egress links are overloaded.
- Check whether traffic of flows of the same client is distributed through the same egress interface based on the source IP address.
- Check the traffic statistics of egress links.
- Check whether MLLB configuration takes effect.

Related Commands

Enabling MLLB

Command	**mllb enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the bandwidth-based policy Function of MLLB

Command	**mllb policy bandwidth**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to balance load based on bandwidth policies to distribute egress traffic of an ECMP according to bandwidth.

Configuring Interface Bandwidth

Command	**bandwidth** *kilobits*
Parameter Description	*kilobits*: Indicates the bandwidth of an interface (unit: kbps).
Command Mode	Interface configuration mode
Usage Guide	Use this command to configure egress bandwidth of an interface.

Defining Weight Value

Command	**mllb interface** *inteface* **weight** *weight-num*
Parameter Description	*inteface*: Indicates an interface name. *weight-num*: Indicates a user-defined weight value (unit: kbps).
Command Mode	Global configuration mode
Usage Guide	Use this command to define weight values.

Configuring the Source IP Address

Command	**mllb load-sharing original**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to ensure that traffic of flows of a client is distributed through the same egress interface. The function is used in conjunction with the bandwidth-based policy function.

Configuring Preferred Link

Command	**mllb first-choice** *interface-type interface-number*
Parameter Description	*interface-type interface-number*: Indicates a preferred interface.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure a preferred interface. If egress traffic exceeds the threshold, the traffic is distributed to the preferred link.

Configuring Load Thresholds

Command	**mllb threshold** { *percent-upper* | [**lower** *percent-lower*] }
Parameter Description	*percent-upper*: Indicates an upper limit of a link. *percent-lower*: Indicates a lower limit of a link. The value ranges from 1 to 100. Default value: 100 (unit: %).
Command Mode	Global configuration mode
Usage Guide	Egress links that exceed the upper limit will not distribute traffic.

Displaying Load Balancing Information of Egress Interface

Command	**show mllb statistics**
Parameter Description	N/A
Command	Privileged EXEC mode, global configuration mode, and interface configuration mode

Mode	
Usage Guide	Use this command to display load balancing information of flows on all egress interfaces.

Displaying MLLB Module Configuration

Command	**show mllb configure**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	Use this command to display MLLB module configuration.

Configuration Example

Creating MLLB Load Balancing Service to Support Bandwidth-based policy Function

Scenario	An Internet café is configured with three ADSL links. The bandwidth of the links is 50 Mbps, 50 Mbps, and 100 Mbps, respectively. The ADSL links are used based on the bandwidth-based policy.
Configuration Steps	● Enable MLLB in global configuration mode. FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# mllb enable ● Configure a default route. FS(config)# ip route 0.0.0.0 0.0.0.0 dialer 1 FS(config)# ip route 0.0.0.0 0.0.0.0 dialer 2 FS(config)# ip route 0.0.0.0 0.0.0.0 dialer 3 ● Configure ADSL link bandwidth. FS(config)#interface dialer 1 FS(config-if-dialer 1)#bandwidth 50000 FS(config-if-dialer 1)# end FS(config)# interface dialer 2 FS(config-if-dialer 2)#bandwidth 50000 FS(config-if-dialer 2)# end FS(config)# interface dialer 3 FS(config-if-dialer 3)#bandwidth 100000 FS(config-if-dialer 3)# end ● Enable the bandwidth-based policy function. FS(config)#mllb policy bandwidth
Verification	Access an external network as a user of the Internet café to display link load information. ● Run the **show mllb configure** command to check whether MLLB configuration takes effect. ● Run the **show mllb statistics** command to display link load information.

Common Errors

- The MLLB switch is not configured. As a result, configuration is invalid.

- The configured egress bandwidth value is inconsistent with the network bandwidth of an ISP. As a result, the balancing result is affected.
- No default route is configured.

9.4.2 Configuring Load-based Policy of MLLB

Configuration Effect

- Balance load based on load policies to distribute traffic of ECMP egress flows to a link with the minimum load.

Notes

- MLLB is effective to ECMP egress flows. Therefore, ECMP must be configured on the network.

Configuration Steps

Enabling MLLB

- Mandatory. Enable MLLB in global configuration mode.

Configuring the load-based policy Function of MLLB

- Mandatory. Configure the load-based policy function in global configuration mode.

Enabling Load Monitoring

- Optional. Use the default configuration to monitor the downlink traffic of the egress links.
- Enable load monitoring in global configuration mode and select the uplink or downlink traffic to be monitored based on actual requirements.

Configuring Preferred Link

- Optional. The function is not enabled by default.
- Configure the preferred link in global configuration mode.

Configuring Load Thresholds

- Optional. The default upper and lower limits of thresholds are 100, respectively.
- Configure the load thresholds in global configuration mode.

Configuring Load Update Period

- Optional. Load is updated every five seconds by default.
- Configure the load update period in global configuration mode.

Verification

Verify that the traffic of ECMP egress flows is distributed according to the policy of MLLB.

- Check whether the egress traffic is distributed based on the load-based policy.
- Check the traffic statistics of egress links.
- Check whether traffic is distributed to the preferred link if all ECMP egress links are overloaded.

- Check whether MLLB configuration takes effect.

Related Commands

Enabling MLLB

Command	**mllb enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Load-based Policy of MLLB

Command	**mllb policy load**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to balance load dynamically according to the load of egress links.

Enabling Load Monitoring

Command	**load-monitor uplink**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to monitor the uplink or downlink load of egress links. Downlink load is monitored by default.

Configuring Load Update Period

Command	**mllb load-interval** *refresh-time*
Parameter Description	*refresh-time*: Indicates the load update period. The value ranges from 3 to 30 (unit: second).
Command Mode	Global configuration mode
Usage Guide	Use this command to periodically update the load of egress links.

Configuration Example

Creating MLLB Load Balancing Service to Support Load-based Policy

Scenario	Three egress links are configured on a campus network. The bandwidth of the links is 50 Mbps, 50 Mbps, and 100 Mbps, respectively. The egress links are used based on the load-based policy.

Configuration Steps	● Enable MLLB in global configuration mode. FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# mllb enable ● Configure a default route. FS(config)# ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/1 202.101.98.54 FS(config)# ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/2 202.101.98.55 FS(config)# ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/3 202.101.98.56 ● Enable the load-based policy. FS(config)#mllb policy load ● Enable the preferred link. FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#mllb first-choice GigabitEthernet 0/1
Verification	Access an external network as a user of the campus network to display link load information. ● Run the **show mllb configure** command to check whether MLLB configuration takes effect. ● Run the **show mllb statistics** command to display link load information.

Common Errors

- The MLLB switch is not configured. As a result, configuration is invalid.
- No default route is configured.
- The configured egress interface of the preferred link is not an ECMP egress interface.

9.4.3 Configuring Automatic Network Detection

Configuration Effect

- Periodically measure the number of half-open connections, delay, and routing traffic information of the current network, check the accessibility of a specified DNS server and domain name, and record data into a database.

Notes

- Domain name accessibility detection and network detection are separately enabled.

Configuration Steps

Enabling Network Detection

- Mandatory. Enable network detection in global configuration mode.

Enabling Domain Name Detection

- Mandatory. Enable domain name detection in global configuration mode.

Configuring IP Address and Interface of DNS Server

- Mandatory. Configure the IP address and interface of the DNS server in global configuration mode.

Configuring Domain Name

- Mandatory. Configure a domain name in global configuration mode.

Configuring Detection Period

- Optional. The default detection period is five minutes.
- Configure the detection period in global configuration mode.

Verification

- Check whether the network detection configuration takes effect.

Related Commands

Enabling Network Detection

Command	**mllb detect network enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling Domain Name Detection

Command	**mllb detect domain enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring IP Address and Interface of DNS Server

Command	**mllb detect domain dns-server** *dns-ip interface* **source-ip** *source-ip-address*
Parameter Description	*dns-ip*: Indicates the IP address of a DNS server. *inteface*: Indicates the name of an egress interface. *source-ip-address*: Indicates the source IP address for detection.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Domain Name

Command	**mllb detect domain add** *domain-name*
Parameter Description	*domain-name*: Indicates a domain name for detection.
Command	Global configuration mode

Mode	
Usage Guide	N/A

Configuring Detection Period

Command	**mllb detect** {**domain** | **network**} **interval** *interval-time*
Parameter Description	*interval-time*: Indicates a detection period. The value ranges from 1 to 1440 (unit: minute).
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring Automatic Network Detection

Scenario	Two egress links are configured on an enterprise network: 100 Mbps Telecom link and 50 Mbps Unicom link. Intranet users access the Internet using the 8.8.8.8 DNS server, and the webpage browsing throughput is low. It is suspected that the Unicom link and the DNS server are faulty. Configure the automatic detection function to check for the problems.
Configuration Steps	● Enable the automatic detection function. FS(config)# mllb detect domain enable FS(config)# mllb detect network enable ● Configure a domain name. FS(config)# mllb detect domain add www.qq.com FS(config)# mllb detect domain add www.tmall.com FS(config)# mllb detect domain add www.jd.com ● Configure the IP address and interface of the DNS server. FS(config)# mllb detect domain dns-server 8.8.8.8 GigabitEthernet 0/1 FS(config)# mllb detect domain dns-server 8.8.8.8 GigabitEthernet 0/2 source-ip 192.168.197.16
Verification	Run the **show mllb detect configure** command to display the configuration result.

Common Errors

- The domain name and network detection functions are not enabled. As a result, configuration is invalid.
- The numbers of domain names and DNS servers reach the upper limit. As a result, new domain name and DNS server fail to be added.

#endif

9.5 Monitoring

Displaying

Description	Command
Displays MLLB configuration.	**show mllb configure**

Displays statistical information of MLLB egress interfaces.	**show mllb statistics**
Displays MLLB detection configuration.	**show mllb detect configure**

10 Configuring USER-ROUTE

10.1 Overview

USER-ROUTE provides a routing policy that provides the egress network service based on user authentication information.

When users of a campus network access a network through multiple egress links, FS gateways can be configured to associate with the Security Accounting Management (SAM) authentication device, so as to provide differentiated network services for different users and resolve the problem that conventional campus network users cannot actively select a network service.

USER-ROUTE supports the "prior line" and "posterior line" network services. A prior line indicates an operator line purchased by students while a posterior line indicates the China Education and Research Network (CERNET) line owned by a university.

USER-ROUTE is applicable to multi-egress networks of different operators, as well as network service scenarios based on user authentication information.

10.2 Applications

Application	Description
Configuring USER-ROUTE for Multi-egress Campus Network	Four external network lines are configured on a campus network, where gigabitEthernet 0/1 and gigabitEthernet 0/2 are lines of China Telecom, gigabitEthernet 0/3 is a line of China Unicom, and gigabitEthernet 0/4 is the CERNET line. There are authenticated users and unauthenticated users in the internal network. The configuration of USER-ROUTE does not take effect on unauthenticated users. Authenticated users can access the CERNET resources via the CERNET. They are charged when accessing resources of China Telecom or China Unicom. Authenticated users of China Telecom can use only the line of China Telecom when accessing public network resources except the CERNET resources. Likewise, users of China Telecom can use only the line of China Unicom when accessing public network resources except the CERNET resources.

10.2.1 Configuring USER-ROUTE for Multi-egress Campus Network

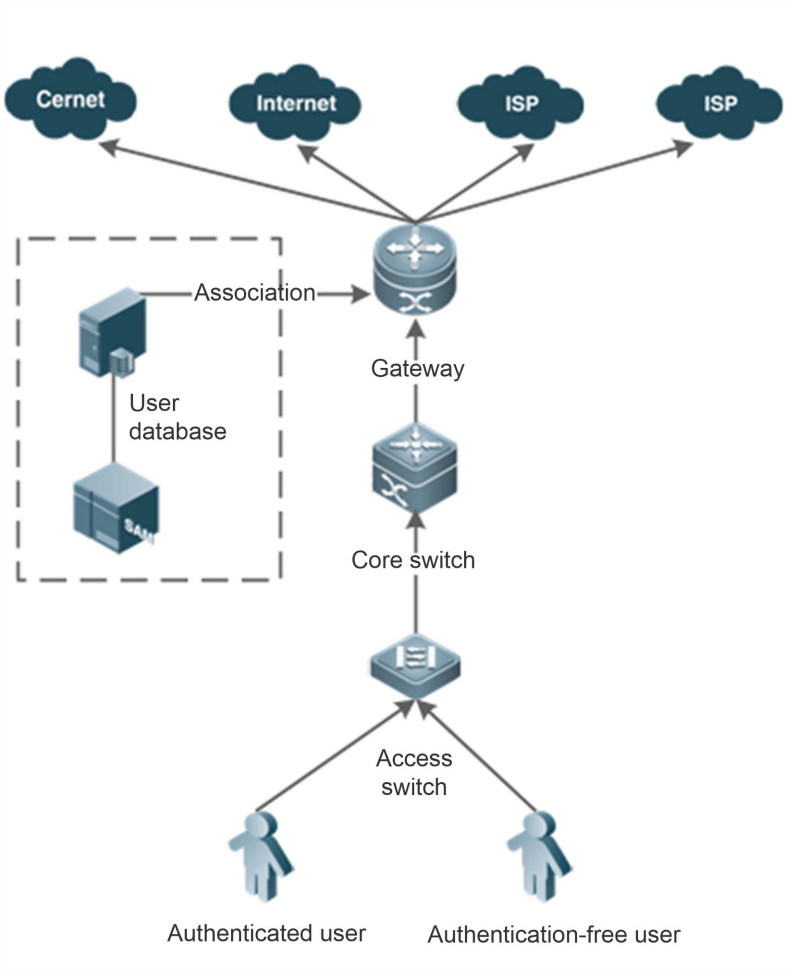
Scenario

Multiple Internet Service Providers (ISPs) provide multilink network services.

As shown in Figure 1-1, China Telecom, China Unicom, and CERNET provide the egress network services for campus network users.

- At least one SAM server is deployed, and internal network users can access the Internet after passing authentication on the SAM server.
- Lines of multiple operators are available in the external network.

Figure 10-1



Deployment

- Identify the prior line and posterior line correctly for users. The prior line of China Telecom users is the line of China Telecom, the prior line of China Unicom users is the line of China Unicom, and the "posterior line" is the CERNET line.
- The posterior line uses the common routing mode. A route database or static routes in an operator network segment need to be configured on the external network port.
- The next hop of an egress needs to be configured on the external network port in advance.
- The user group name needs to be consistent with the name in the egress control policy of the SAM server.
- Enable the SAM association function.

USER-ROUTE does not support routing for unauthenticated users. The common routing mode is adopted for authenticated users, their packets are routed to the posterior line, and the posterior line is used preferentially. Otherwise, the prior line is used. If exit restriction is enabled, when both the prior line and posterior line are unavailable, user traffic is discarded. Otherwise, user traffic is forwarded to other routing modules for processing.

For details about the SAM association function, see the *LINK-SAM-SCG* and *LINK-SAM-CREF*.

10.3 Features

Basic Concepts

Flow

Flows or flow sessions are packets with the same 5-tuple (source and destination IP addresses, source and destination ports, and protocol ID) within a period of time.

Authenticated User

Authenticated users are internal network users who pass Web authentication or 802.1X authentication of FS products before they access the Internet. After users pass authentication, their identity information and relevant charging mode are stored in FS authentication and charging system, that is, the SAM server. FS SAM server supports one IP address for one user.

User Group

A user group is a collection of a series of IP addresses. Each user group has one name. Access control policies such as prior line or posterior line can be configured for each user group. USER-ROUTE selects routes according to the prior line and posterior line configured in user groups. After routing is completed, other routing modules no longer route the packets.

SAM Association

USER-ROUTE shares information about authenticated users with the SAM server. If an authenticated user is online, the SAM server sends the IP address and user group information of the user to the L2/L3 class identification module of the gateway.

User Information

When a user goes online after passing 802.1X authentication or Web authentication, if SAM association is enabled, the SAM server delivers the user information to the L2/L3 class identification module of the gateway. Online user information includes the IP address and user group information of an online user.

Prior Line

A prior line is public network line resources purchased by an authenticated user. It generally refers to an operator line. For example, if a student purchases the Internet access package of China Telecom, the prior line of the student is the line of China Telecom. Likewise, if a student purchases the Internet access package of China Unicom, the prior line of the student is the line of China Unicom. The next hop needs to be configured on the interface of a prior line.

Posterior Line

A posterior line is the line whose resources can be accessed by authenticated users without purchase, for example, the CERNET line. The next hop and route database or static routes need to be configured on the interface of the posterior line.

Load Balancing

When the prior line has multiple egresses, the load of the prior line is balanced based on bandwidth by default. When the posterior line has multiple egresses, load balancing is disabled by default but it can be enabled.

Exit Restriction

Exit restriction for packets is to prohibit users who are not authorized to access a resource from accessing the resource. USER-ROUTE does not perform exit restriction on packets by default but a command can be executed to configure exit restriction for packets.

Overview

Feature	Description

USER-ROUTE Switch	Enables/Disables USER-ROUTE.
User Group	Creates a user group for USER-ROUTE.
Prior Line	Configures an egress for a prior line. If there are multiple egresses, multiple prior lines can be configured. A maximum of 32 prior lines can be configured.
Posterior Line	Configures an egress for a posterior line. If there are multiple egresses, multiple posterior lines can be configured. A maximum of 32 posterior lines can be configured.
Load Balancing	Enables load balancing for posterior lines.
Load Balancing Hash Factor	Configures a load balancing hash factor. The load balancing hash factor can be based on source IP address, source IP address + destination IP address, or destination IP address.
Exit Restriction	Configures the exit restriction function in the case of a routing failure.

10.3.1 USER-ROUTE Switch

The user route switch is used to enable or disable USER-ROUTE.

Working Principle

When user route switch is enabled, flows are routed by USER-ROUTE.

When user route switch is disabled, flows are not routed by USER-ROUTE.

Related Configuration

- Enabling USER-ROUTE

By default, USER-ROUTE is disabled on FS gateways.

Run the **user-route enable** command in global configuration mode to enable USER-ROUTE.

- Disabling USER-ROUTE

By default, USER-ROUTE is disabled on FS gateways.

To disable USER-ROUTE, run the **no user-route enable** command in global configuration mode.

10.3.2 User Group

USER-ROUTE selects routes based on user groups. The user group name configured on the gateway needs to be consistent with the user group name on the SAM server.

Working Principle

USER-ROUTE selects proper egress lines based on user group information.

Related Configuration

- Configuring User Group

No user group is configured by default.

Run the **user-route user-group** *user-group-name* command in global configuration mode to configure a user group.

- Deleting User Group

Run the **no user-route user-group** *user-group-name* command in global configuration mode to delete a user group.

10.3.3 Prior Line

A prior line needs to be configured for USER-ROUTE before USER-ROUTE is used.

Working Principle

When data flows match a user group of USER-ROUTE, the data flows are routed to an egress according to the prior line configured in the user group.

Related Configuration

Configuring Prior Line for Users

Run the **prior-line interface** *interface-name* command in global configuration mode to configure a prior line for users.

Run the **no prior-line interface** *interface-name* command in global configuration mode to disable a prior line.

The next hop needs to be configured on the interface of a prior line.

10.3.4 Posterior Line

If a line can be used as a posterior line, the posterior line needs to be configured.

Working Principle

When data flows match a user group of USER-ROUTE, the data flows are routed to an egress according to the posterior line configured in the user group.

Related Configuration

Configuring Posterior Line for Users

Run the **posterior -line interface** *interface-name* command in global configuration mode to configure a posterior line for users.

Run the **no posterior -line interface** *interface-name* command in global configuration mode to disable the posterior line.

The next hop and route database or static routes need to be configured on the interface of a posterior line.

10.3.5 Load Balancing

If multiple posterior lines are from the same operator, the load balancing function can be enabled for them.

Working Principle

After load balancing is enabled for posterior lines, data flows are routed to egresses according to the load balancing policy (bandwidth-based policy by default).

Related Configuration

Configuring Load Balancing Function for Posterior Lines

By default, the load balancing policy for posterior lines is disabled on USER-ROUTE of FS gateways.

Run the **user-route posterior-line load-balance enable** command in global configuration mode to enable the load balancing function for posterior lines on USER-ROUTE.

Run the **no user-route posterior-line load-balance enable** command in global configuration mode to disable the load balancing function.

10.3.6 Load Balancing Hash Factor

By default, the load balancing algorithm uses source IP addresses in hashing. If the hash effect is unsatisfactory, you can change the hash factor to destination IP address or destination IP address + source IP address.

Working Principle

Data flows are routed to egresses according to the load balancing policy based on the load balancing hash factor.

Related Configuration

↘ Configuring Load Balancing Hashing for Posterior Lines

By default, the load balancing hash factor of USER-ROUTE is based on the source IP address on FS gateways.

Run the **user-route load-sharing destination** command in global configuration mode to enable the destination IP address-based load balancing hashing for USER-ROUTE.

Run the **user-route load-sharing destination-original** command in global configuration mode to enable the load balancing hashing based on source IP address + destination IP address for USER-ROUTE.

Run the **no user-route load-sharing** command in global configuration mode to restore the source IP address-based load balancing hashing.

10.3.7 Exit Restriction

In general, the gateway does not restrict the user access to an external network. The exit restriction is completed by the exit device of FS, for example, the ACE device has the exit restriction function. In scenarios in which no exit device such as ACE is available, if the exit restriction function needs to be enabled on the gateway, run this command. For example, if a user in a user group is authorized to access the internal network but has no permission to access the external network, this command can be configured for such users. In addition, if a line of a user group malfunctions and as a result, the configured prior line is unavailable for the packets, USER-ROUTE cannot route packets by default. The exit restriction function can enable other routing modules to route the packets. If packets do not need to be routed by other routing modules, run this command.

Working Principle

When data flows fail to be routed by USER-ROUTE, if the exit restriction function is enabled, the data flows will be discarded by USER-ROUTE.

Related Configuration

↘ Configuring Exit Restriction Function

By default, the exit restriction function of USER-ROUTE is disabled on FS gateways.

Run the **deny others** command in user group configuration mode to enable the exit restriction function for a user group of USER-ROUTE.

Run the **no deny others** command in user group configuration mode to disable the exit restriction function.

10.3.8 Forward DNS Proxy Association

Assume that an internal network user is a user of operator A but the Domain Name Service (DNS) server configured for the user is of Operator B or C. After the USER-ROUTE switch is enabled, packets from the user are sent out along the line of Operator A but most addresses parsed by the DNS server are network addresses of Operator B or C. Consequently, cross-operator network access will be incurred, which may result in long delay in web page access and a failure to open Web pages. The forward DNS proxy function can intercept DNS request packets from the internal network, and change the destination IP address in DNS request packets based on the bandwidth or load of the current egress, thereby achieving transparency of the DNS configuration of the internal network. After USER-ROUTE is enabled, it is recommended that the forward DNS proxy function be enabled. Note that the forward DNS proxy function needs to be applied to all egresses of USER-ROUTE.

Working Principle

After both USER-ROUTE and the forward DNS proxy function are enabled, an association function becomes available between them. That is, after intercepting a DNS request packet from a user, the forward DNS proxy function queries the egress configuration of the user. If the user is a China Telecom user, the DNS request packet from the user is routed to the specified egress of China Telecom for DNS processing. The association function achieves transparency of the DNS server configuration of internal network users and effectively prevents cross-operator network access, thereby improving Internet access experience for users.

Related Configuration

By default, the forward DNS proxy function is disabled.

For details about how to enable the DNS proxy function, see DNS-PROXY-SCG.

Note that the forward DNS proxy needs to be configured on all egresses specified for USER-ROUTE, the association function does not need to be configured additionally, and the association is automatically performed internally.

10.4 Configuration

Configuration	Description and Command	
Configuring USER-ROUTE	(Mandatory) It is used to configure the routing service for USER-ROUTE.	
	user-route enable	Enables USER-ROUTE.
	link-sam enable	Enables SAM association.
	user-route user-group *user-group-name*	Configures a user group.
	prior-line interface *interface-name*	Configures a prior line.
	posterior -line interface *interface-name*	Configures a posterior line.
	nexthop *ip-address*	Configures the next-hop gateway for an egress.
	(Optional) It is used to configure the exit, load balancing, and other services.	
	deny others	Configures the exit restriction function.
	user-route posterior-line load-balance enable	Configures the load balancing function for posterior lines.

	user-route load-sharing [destination |original | destination-original]	Configures the load balancing hash factor that is based on source IP address, destination IP address, or source IP address + destination IP address. The default load balancing hash factor is based on source IP address.
	link-sam protocol { v1 | v2 }	Configures a protocol version for the SAM module. The default protocol version is v2(3.9.0).
	link-sam port *port*	Configures a TCP port for SAM association. The default value is 2012.
	link-sam conn-timeout *minutes*	Configures the SAM association timeout period. The default value is 20 minutes and the value ranges from 20 to 150,000.

10.4.1 Configuring USER-ROUTE

Configuration Effect

Enable USER-ROUTE to route data flows.

Notes

- Only the EG2000XE, EG2000X, and EG2000UE support USER-ROUTE. Other EG devices, NBR, AG, and other gateways do not support USER-ROUTE.
- Information about a configured user group needs to be consistent with that on the SAM server.
- The next hop needs to be configured for prior lines and posterior lines.

Configuration Steps

Enabling USER-ROUTE

- Mandatory. Perform the configuration in global configuration mode.

Enabling SAM Association

- Mandatory. Perform the configuration in global configuration mode.

Configuring User Group for USER-ROUTE

- Mandatory. Perform the configuration in global configuration mode.

Configuring Prior Line

- Mandatory. In user group configuration mode, configure an egress for the prior line.

Configuring Posterior Line

- Mandatory. In user group configuration mode, configure an egress for the posterior line.

Configuring Next-hop Gateway for Egress

- Mandatory. In interface configuration mode, configure the next hop according to the actual egress.

Configuring Exit Restriction Function

- Optional. The exit restriction function is disabled by default. If exit restriction is required for users, the function must be configured.
- Perform the configuration in global configuration mode.

Configuring Load Balancing Function for Posterior Lines

- Optional. The load balancing function is disabled by default. If load balancing is required for posterior lines, the function must be configured.
- Perform the configuration in global configuration mode.

Configuring Load Balancing Hash Factor

- Optional. The load balancing hashing is based on source IP address by default.
- To configure load balancing hashing that is based on source IP address + destination IP address, run the **user-route load-sharing destination-original** command.
- To configure load balancing hashing that is based on destination IP address, run the **user-route load-sharing destination** command.
- Perform the configuration in global configuration mode.

Configuring Protocol Version for SAM Module

- Optional. The default protocol version is v2(3.9.0). If the protocol version needs to be changed, it must be configured.
- Perform the configuration in global configuration mode. After the function is configured, a protocol earlier than SAM v2(3.9.0) is used.

Configuring TCP Port for SAM Association

- Optional. The default port ID is 2012. If the port ID needs to be changed, the TCP port for SAM association must be configured.
- Perform the configuration in global configuration mode.

Configuring SAM Association Timeout Period

- Optional. The default timeout period is 20 minutes. If the timeout period needs to be changed, it must be configured.
- Perform the configuration in global configuration mode.

Verification

Enable data flows in a network to be routed to an egress according to the configuration of USER-ROUTE.

- Check whether data flows of different users are routed according to the configuration of USER-ROUTE.
- Check whether exit restriction is conducted after USER-ROUTE fails to route data flows.
- When loading balancing hashing is based on source IP address, check whether data flows from the same user are routed to the same egress.
- Check the configuration of USER-ROUTE.
- Check the SAM association statistics.

Related Commands

Enabling USER-ROUTE

Command	**user-route enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	USER-ROUTE needs to be enabled before it is used. After enabled, USER-ROUTE listens to and accepts the SAM connection, and then receives online user information from the SAM server.

Enabling SAM Association

Command	**link-sam enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	USER-ROUTE relies on online user information delivered by the SAM server. Therefore, before enabling USER-ROUTE, enable the SAM association function so that USER-ROUTE receives online user information delivered by the SAM server.

Configuring User Group

Command	**user-route user-group** *user-group-name*
Parameter Description	*user-group-name*: Indicates the name of a user group. The value can contain a maximum of 30 characters.
Command Mode	Global configuration mode
Usage Guide	The user route priority is as follows: Policy-Based Routing (PBR) > user routing > application routing > common routing. USER-ROUTE routes data flows according to the prior line and posterior line configured in a user group. After routing is completed, other routing modules no longer route the data flows. A maximum of 64 user groups can be configured.

Configuring Prior Line

Command	**prior-line interface** *interface-name*
Parameter Description	*interface-name*: Indicates the interface name of a prior line.
Command Mode	User group configuration mode
Usage Guide	The next hop needs to be configured for the egress of a prior line. A user group supports a maximum of 32 prior lines.

Configuring Posterior Line

Command	**posterior -line interface** *interface-name*
Parameter Description	*interface-name*: Indicates the interface name of a posterior line.
Command Mode	User group configuration mode
Usage Guide	The next hop and route database need to be configured for the egress of a posterior line. A user group supports a maximum of 32 posterior lines.

Configuring Next-hop Gateway for Egress

Command	**nexthop** *ip-address*
Parameter Description	*ip-address*: Indicates the next-hop IP address of an egress.
Command Mode	Interface configuration mode
Usage Guide	Use this command to configure the next-hop gateway for an egress.

Configuring Exit Restriction Function

Command	**deny others**
Parameter Description	*N/A*
Command Mode	User group configuration mode
Usage Guide	In general, the gateway does not restrict the user access to an external network. The exit restriction is completed by the exit device of FS, for example, the ACE device has the exit restriction function. In scenarios in which no exit device such as ACE is available, if the exit restriction function needs to be enabled on the gateway, run this command. For example, if a user in a user group is authorized to access the internal network but has no permission to access the external network, this command can be configured for such users. In addition, if a line of a user group malfunctions and as a result, the configured prior line is unavailable for the packets, USER-ROUTE cannot route packets by default. The exit restriction function can enable other routing modules to route the packets. If packets do not need to be routed by other routing modules, use this command.

Configuring Load Balancing Function for Posterior Lines

Command	**user-route posterior-line load-balance enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, the load balancing is disabled for posterior lines. If there are multiple posterior lines, and these posterior lines are from the same operator or the cross-network access is not slow, the load balancing can be enabled. Load balancing is a bandwidth-based policy.

Configuring Load Balancing Hash Factor

Command	**user-route load-sharing** [**destination** | **original** | **destination-original**]
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, USER-ROUTE conducts hashing by using the source IP address for load balancing. In this way, the traffic of the same user is balanced to the same egress. If load balancing based on source IP address is unsatisfactory, you can configure the destination IP address-based load balancing or load balancing based on source IP address + destination IP address.

Displaying Configuration of USER-ROUTE

Command	**show user-route** [**user-group** *user-group-name*] **configure**
Parameter Description	*user-group-name*: Indicates the name of a user group. The value can contain a maximum of 30 characters.
Command Mode	Global configuration mode and privileged EXEC mode
Usage Guide	If no user group is specified, the configurations of all user groups are displayed by default. If a user group is specified, the configuration of the user group is displayed.

Configuring Protocol Version of SAM Module

Command	**link-sam protocol old**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	When deploying the SAM association function, network administrators need to check the current version of the SAM module to prevent a communication failure caused by unmatched protocol versions. To display the version of the SAM module, enable the SAM association function, run the **show link-sam statistics** command, and check whether the value of the **exception messages** field increases substantially. If yes, a protocol version inconsistency occurs.

Configuring TCP Port for SAM Association

Command	**link-sam port** *port*
Parameter Description	*port*: Specifies the TCP port ID.
Command Mode	Global configuration mode
Usage Guide	In general, the default port ID is used.

Configuring SAM Association Timeout Period

Command	**link-sam conn-timeout** *minutes*

Parameter Description	*minutes*: Indicates the association timeout period (unit: minute). The value ranges from 20 to 150,000.
Command Mode	Global configuration mode
Usage Guide	The association timeout period is generally set to the default value (20 minutes).

Displaying SAM Association Statistics

Command	**show link-sam statistics**
Parameter Description	N/A
Command Mode	Global configuration mode and privileged EXEC mode
Usage Guide	Display the association statistics of the SAM server associated with USER-ROUTE.

Configuration Example

Configuring USER-ROUTE in Network

Scenario	Four external network lines are configured on a campus network, where gi0/1 and gi0/2 are lines of China Telecom, gi0/3 is a line of China Unicom, and gi0/4 is the CERNET line.
Configuration Steps	● Enable the multilink load balancing function globally. FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# user-route enable ● Configure a route database. FS(config)# route-auto-choose cernet GigabitEthernet 0/4 219.243.240.5 ● Configure an egress gateway. FS(config)#interface GigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)#nexthop 120.35.31.101 FS(config)#interface GigabitEthernet 0/2 FS(config-if-GigabitEthernet 0/2)#nexthop 120.35.31.108 FS(config)#interface GigabitEthernet 0/3 FS(config-if-GigabitEthernet 0/3)#nexthop 58.22.122.110 FS(config)#interface GigabitEthernet 0/4 FS(config-if-GigabitEthernet 0/4)#nexthop 219.243.240.5 ● Configure a user group. FS(config)#mllb policy bandwidth # Configure a user group for China Telecom users. FS(config)#user-route user-group cnii # Configure a prior line of China Telecom. FS(config-user-group)#prior-line GigabitEthernet0/1 FS(config-user-group)#prior-line GigabitEthernet0/2 # Configure a posterior line for the user group. FS(config-user-group)#posterior-line GigabitEthernet0/4

	# Configure a user group for China Unicom users. FS(config)#user-route user-group cnc # Configure a prior line of China Unicom. FS(config-user-group)#prior-line GigabitEthernet0/3 # Configure a posterior line for the user group. FS(config-user-group)#posterior-line GigabitEthernet0/4 ● Configure SAM association. # Enable the SAM association. FS(config)#link-sam enable
Verification	Enable campus network users to access an external network. ● Run the **show user-route configure** command to display the configuration of USER-ROUTE. ● Run the **show link-sam statistics** command to display SAM association information.

Common Errors

- The SAM association is not configured.
- No egress gateway is configured.

10.5 Monitoring

Clearing

Description	Command
Clears SAM statistics.	**clear link-sam statistics**

Displaying

Description	Command
Displays the configuration of USER-ROUTE.	**show user-route** [**user-group** *user-group-name*] **configure**
Displays the SAM association statistics.	**show link-sam statistics**

Chapter 7 IPv6 Configuration

1. Configuring IPv6

1 Configuring IPv6

1.1 Overview

As the Internet develops rapidly and IPv4 address space is becoming exhausted, IPv4 limitations become more and more obvious. At present, many researches and practices on Internet Protocol Next Generation (IPng) have been conducted. The IPng working group of the Internet Engineering Task Force (IETF) has formulated an IPng protocol named IP Version 6 (IPv6), which is described in RFC 2460.

Main Features

- **Larger Address Space**

Compared with 32 bits in an IPv4 address, the length of an IPv6 address is extended to 128 bits. Therefore, the address space has approximately 2^{128} addresses. IPv6 adopts a hierarchical address allocation mode to support address allocation of multiple subnets from the Internet core network to intranet subnet.

- **Simpler Packet Header Format**

Since the design principle of the IPv6 packet header is to minimize the overhead of the packet header, some non-key fields and optional fields are removed from the packet header to the extended packet header. Therefore, although the length of an IPv6 address is four times of that of an IPv4 address, the IPv6 packet header is only two times of the IPv4 packet header. The IPv6 packet header makes device forwarding more efficient. For example, with no checksum in the IPv6 packet header, the IPv6 device does not need to process fragments (fragmentation is completed by the initiator).

- **Efficient Hierarchical Addressing and Routing Structure**

IPv6 uses a convergence mechanism and defines a flexible hierarchical addressing and routing structure. Multiple networks at the same layer are represented as a uniform network prefix on the upstream device, greatly reducing routing entries maintained by the device and routing and storage overheads of the device.

- **Easy Management: Plug and Play (PnP)**

IPv6 provides automatic discovery and auto-configuration functions to simplify management and maintenance of network nodes. For example, Neighbor Discovery (ND), MTU Discovery, Router Advertisement (RA), Router Solicitation (RS), and auto-configuration technologies provide related services for PnP. Particularly, IPv6 offers two types of auto-configuration: stateful auto-configuration and stateless auto-configuration. In IPv4, Dynamic Host Configuration Protocol (DHCP) realizes auto-configuration of the host IP address and related parameters. IPv6 inherits this auto-configuration service from IPv4 and called it stateful auto-configuration (see DHCPv6). Besides, IPv6 also offers the stateless auto-configuration service. During stateless auto-configuration, a host automatically obtains the local address of the link, address prefix of the local device, and other related configurations.

- **Security**

As an optional extension protocol of IPv4, Internet Protocol Security (IPSec) is a part of IPv6 to provide security for IPv6 packets. At present, IPv6 provides two mechanisms: Authentication Header (AH) and Encapsulated Security Payload (ESP). AH provides data integrity and authenticates IP packet sources to ensure that the packets originate from the nodes identified by the source addresses. ESP provides data encryption to realize end-to-end encryption.

Better QoS Support

A new field in the IPv6 packet header defines how to identify and process data streams. The Flow Label field in the IPv6 packet header is used to authenticate a data flow. Using this field, IPv6 allows users to propose requirements on the communication quality. , A device can identify all packets belonging to a specific data stream based on this field and process these packets according to user requirements.

New Protocol for Neighboring Node Interaction

IPv6 Neighbor Discovery Protocol (NDP) uses a series of Internet Control Message Protocol Version 6 (ICMPv6) packets to implement interactive management of neighboring nodes (nodes on the same link). IPv6 uses NDP packets and efficient multicast/unicast ND packets instead of broadcast-based Address Resolution Protocol (ARP) and Control Message Protocol Version 4 (ICMPv4) router discovery packets.

Extensibility

With strong extensibility, IPv6 features can be added to the extended packet header following the IPv6 packet header. Unlike IPv4, the IPv6 packet header can support at most 40 bytes of options. For an IPv6 packet, the length of the extended packet header is restricted only by the maximum number of bytes in the packet.

Protocols and Standards

RFC 4291 - IP Version 6 Addressing Architecture
RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification
RFC 4443 - Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
RFC 4861 - Neighbor Discovery for IP version 6 (IPv6)
RFC 4862 - IPv6 Stateless Address Auto-configuration
RFC 5059 - Deprecation of Type 0 Routing Headers in IPv6

1.2 Applications

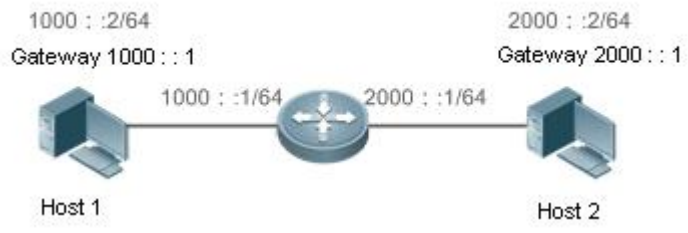
Application	Description
Communication Based on IPv6 Addresses	Two PCs communicate with each other using IPv6 addresses.

1.2.1 Communication Based on IPv6 Addresses

Scenario

As shown in Figure 1-1, Host 1 and Host 2 communicate with each other using IPv6 addresses.

Figure 1-1



Deployment

Hosts can use the stateless address auto-configuration or DHCPv6 address assignment mode. After addresses are configured, hosts can communicate with each other using IPv6 addresses.

1.3 Features

Overview

Feature	Description
IPv6 Address Format	The IPv6 address format makes IPv6 have a larger address space and flexible representation approach.
IPv6 Address Type	IPv6 identifies network applications based on addresses.
IPv6 Packet Header Format	IPv6 simplifies the fixed and extended packet headers to improve the data packet processing and forwarding efficiency of the device.
IPv6 PMTUD	A host dynamically discovers and adjusts the MTU size on the data Tx path, saving router resources and improving IPv6 network efficiency.
IPv6 Neighbor Discovery	ND functions include router discovery, prefix discovery, parameter discovery, address auto-configuration, address resolution (like ARP), next-hop determination, Neighbor Unreachability Detection (NUD), Duplicate Address Detection (DAD), and redirection.
IPv6 Source Routing	This feature is used to specify the intermediate nodes that a packet passes through along the path to the destination address. It is similar to the IPv4 loose source routing option and loose record routing option.
Restricting the Sending Rate of ICMPv6 Error Messages	This feature prevents DoS attacks.
IPv6 HOP-LIMIT	This feature prevents useless unicast packets from being unlimitedly transmitted on the network and wasting network bandwidth.
Refraining from Sending NS Packets to Authentication VLANs	In gateway authentication mode, a device is refrained from sending NS packets to authentication VLANs.
Default Gateway on the Management Interface	The default gateway is configured on the management interface to generate a default route for this interface.

1.3.1 IPv6 Address Format

An IPv6 address is represented in the X:X:X:X:X:X:X:X format, where X is a 4-digit hexadecimal integer (16 bits). Each address consists of 8 integers, with a total of 128 bits (each integer contains 4 hexadecimal digits and each digit contains four bits). The following are three valid IPv6 addresses:

2001:ABCD:1234:5678:AAAA:BBBB:1200:2100

800:0:0:0:0:0:0:1

1080:0:0:0:8:800:200C:417A

These integers are hexadecimal, where A to F represent 10 to 15. Each integer in the address must be represented, except the leading zeros in each integer. If an IPv6 address contains a string of zeros (as shown in the second and third examples above), a double colon (::) can be used to represent these zeros. That is, 800:0:0:0:0:0:0:1 can be represented as 800::1.

A double colon indicates that this address can be extended to a complete 128-bit address. In this approach, only when the 16-bit integers are all 0s, can they can be replaced with a double colon. A double colon can exist once in an IPv6 address.

In IPv4/IPv6 mixed environment, an address has a mixed representation. In an IPv6 address, the least significant 32 bits can be used to represent an IPv4 address. This IPv6 address can be represented in a mixed manner, that is, X:X:X:X:X:X:d.d.d.d, where X is a hexadecimal integer and d is a 8-bit decimal integer. For example, 0:0:0:0:0:0:192.168.20.1 is a valid IPv6 address. It can be abbreviated to ::192.168.20.1. Typical applications are IPv4-compatible IPv6 addresses and IPv4-mapped IPv6 addresses. If the first 96 bits are 0 in an IPv4-compatible IPv6 address, this address can be represented as ::A.B.C.D, e.g., ::1.1.1.1. IPv4-compatible addresses have been abolished at present. IPv4-mapped IPv6 addresses are represented as ::FFFF:A.B.C.D to represent IPv4 addresses as IPv6 addresses. For example, IPv4 address 1.1.1.1 mapped to an IPv6 address is represented as ::FFFF:1.1.1.1.

Since an IPv6 address is divided into two parts: subnet prefix and interface ID, it can be represented as an address with an additional value according to an address allocation method like Classless Inter-Domain Routing (CIDR). The additional value indicates how many bits (subnet prefix) in the address represent the network part. That is, the IPv6 node address contains the prefix length. The prefix length is separated from the IPv6 address by a slash. For example, in 12AB::CD30:0:0:0:0/60, the prefix length used for routing is 60 bits.

Related Configuration

Configuring an IPv6 Address

No IPv6 address is configured on interfaces by default.
Run the ipv6 address command to configure an IPv6 address on an interface.
After configuration, a host can communicate with others using the configured IPv6 address based on DAD.
Run the ipv6 unnumbered command to configure an interface to borrow the IPv6 unicast address of anther interface. This address can be used as the source address of locally sent packets.

1.3.2 IPv6 Address Type

RFC 4291 defines three types of IPv6 addresses:

Unicast address: ID of a single interface. Packets destined to a unicast address are sent to the interface identified by this address.
Multicast address: ID of an interface group (the interfaces generally belong to different nodes). Packets destined to a multicast address are sent to all interfaces included in this address.
Anycast address: ID of an interface group. Packets destined to an anycast address are sent to one interface included in this address (the nearest interface according to the routing protocol).

IPv6 does not define broadcast addresses.

These three types of addresses are described as follows:

Unicast Addresses

Unicast addresses fall into five types: unspecified address, loopback address, link-local address, site-local address, and global unicast address. At present, site-local addresses have been abolished. Except unspecified, loopback, and link-local addresses, all other addresses are global unicast addresses.

Unspecified address

The unspecified address is 0:0:0:0:0:0:0:0, which is usually abbreviated to ::. It has two general purposes:

1. If a host has no unicast address when started, it uses the unspecified address as the source address to send an RS packet to obtain prefix information from the gateway and thereby generate a unicast address.
2. When an IPv6 address is configured for a host, the device detects whether the address conflicts with addresses of other hosts in the same network segment and uses the unspecified address as the source address to send a Neighbor Solicitation (NS) packet (similar to a free ARP packet).

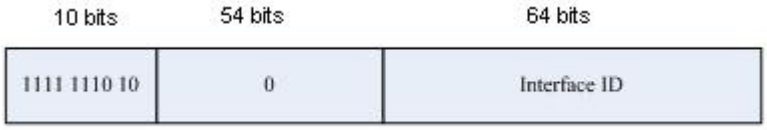
Loopback address

The loopback address is 0:0:0:0:0:0:0:1, which is usually abbreviated to ::1. Similar to IPv4 address 127.0.0.1, the loopback address is generally used by a node to send itself packets.

Link-local address

The format of a link-local address is as follows:

Figure 1- 2

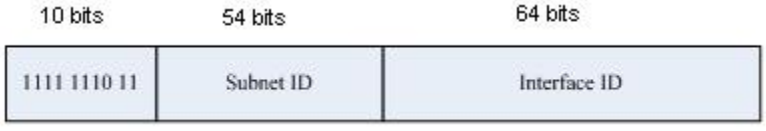


The link-local address is used on a single network link to assign IDs to hosts. The address identified by the first 10 bits in the prefix is the link-local address. A device never forwards packets in which the source or destination address contains the link-local address. The intermediate 54 bits in the address are all 0s. The last 64 bits represent the interface ID, which allows a single network to connect 2^{64}-1 hosts.

Site-local address

The format of a site-local address is as follows:

Figure 1- 3

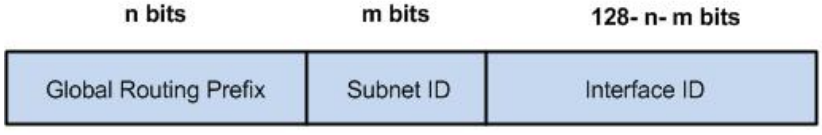


A site-local address is used to transmit data within a site. A device never forwards packets in which the source or destination address contains the site-local address to the Internet. That is, these packets can be forwarded only within the site. A site can be assumed as an enterprise's local area network (LAN). Such addresses are similar to IPv4 private addresses such as 192.168.0.0/16. RFC 3879 has abolished site-local addresses. New addresses do not support the first 10 bits as the prefix and are all regarded as global unicast addresses. Existing addresses can continue to use this prefix.

Global unicast address

The format of a global unicast address is as follows:

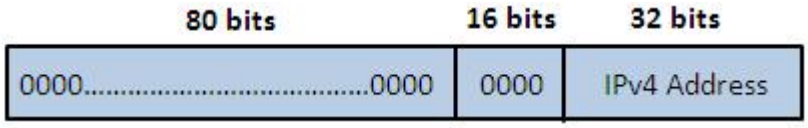
Figure 1- 4



Among global unicast addresses, there is a type of IPv4-embedded IPv6 addresses, including IPv4-compatible IPv6 addresses and IPv4-mapped IPv6 addresses. They are used for interconnection between IPv4 nodes and IPv6 nodes.

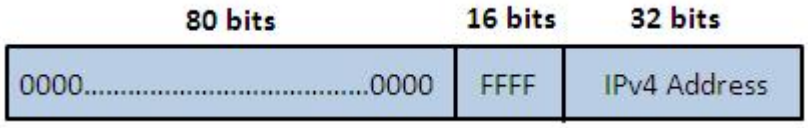
The format of an IPv4-compatible IPv6 address is as follows:

Figure 1- 5



The format of an IPv4-mapped IPv6 address is as follows:

Figure 1- 6



IPv4-compatible IPv6 addresses are mainly used on automatic tunnels. Nodes on automatic tunnels support both IPv4 and IPv6. Using these addresses, IPv4 devices transmit IPv6 packets over tunnels. At present, IPv4-compatible IPv6 addresses have been abolished. IPv4-mapped IPv6 addresses are used by IPv6 nodes to access IPv4-only nodes. For example, if the IPv6 application on an IPv4/IPv6 host requests to resolve the name of an IPv4-only host, the name server dynamically generates an IPv4-mapped IPv6 address and returns it to the IPv6 application.

↘ Multicast Addresses

The format of an IPv6 multicast address is as follows:

```
|    8      |   4 |   4 |                    112 bits                    |
+--------+----+----+-------------------------------------------+
|11111111|flgs|scop|                    group ID                    |
+--------+----+----+-------------------------------------------+
```

The first byte in the address is all 1s, representing a multicast address.

Flag field

The flag field consists of four bits. Currently only the fourth bit is specified to indicate whether this address is a known multicast address assigned by the Internet Assigned Numbers Authority (IANA) or a temporary multicast address in a certain scenario. If the flag bit is 0, this address is a known multicast address. If the flag bit is 1, this address is a temporary multicast address. The remaining three flag bits are reserved for future use.

Scope field

The scope field consists of four bits to indicate the multicast range. That is, a multicast group includes the local node, local link, local site, and any node in the IPv6 global address space.

Group ID field

The group ID consists of 112 bits to identify a multicast group. A multicast ID can represent different groups based on the flag and scope fields.

IPv6 multicast addresses are prefixed with FF00::/8. One IPv6 multicast address usually identifies interfaces on a series of different nodes. After a packet is sent to a multicast address, the packet is then forwarded to the interfaces on each node identified by this multicast address. For a node (host or device), you must add the following multicast addresses:

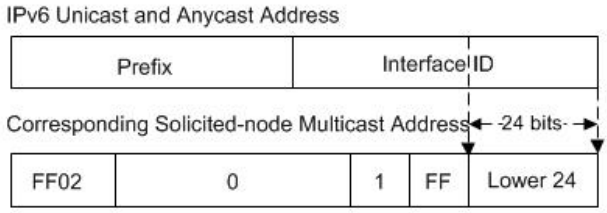
1. Multicast address for all nodes on the local link, that is, FF02::1
2. Solicited-node multicast address, prefixed with FF02:0:0:0:0:1:FF00:0000/104

If the node is a device, it also has to be added to the multicast address of all devices on the local link, that is, FF02::2.

The solicited-node multicast address corresponds to the IPv6 unicast and anycast address. You must add a corresponding solicited-node multicast address for each configured unicast and anycast address of an IPv6 node. The solicited-node multicast address is prefixed with FF02:0:0:0:0:1:FF00:0000/104. The remaining 24 bits are composed of the least significant 24 bits of the unicast or anycast address. For example, if the unicast address is FE80::2AA:FF:FE21:1234, the solicited-node multicast address is FF02::1:FF21:1234.

The solicited-node multicast address is usually used in NS packets. Its address format is as follows:

Figure 1- 7



Anycast Addresses

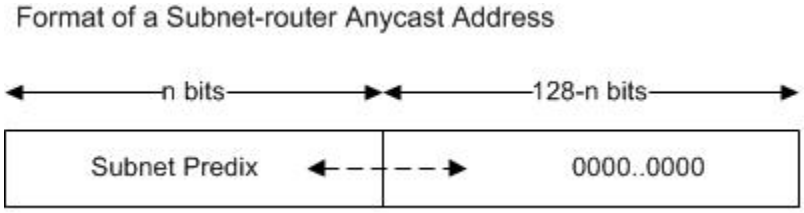
Similar to a multicast address, an anycast address can also be shared by multiple nodes. The difference is that only one node in the anycast address receives data packets while all nodes included in the multicast address receive data packets. Since anycast addresses are allocated to the normal IPv6 unicast address space, they have the same formats with unicast addresses. Every member in an anycast address must be configured explicitly for easier recognition.

Anycast addresses can be allocated only to devices and cannot be used as source addresses of packets.

RFC 2373 redefines an anycast address called subnet-router anycast address. Figure 1- 8 shows the format of a subnet-router anycast address. Such an address consists of the subnet prefix and a series of 0s (interface ID).

The subnet prefix identifies a specified link (subnet). Packets destined to the subnet-router anycast address will be forwarded to a device on this subnet. A subnet-router anycast address is usually used by the application on a node to communicate with a device on a remote subnet.

Figure 1- 8



Related Configuration

Configuring an IPv6 Address

No IPv6 address is configured on interfaces by default.

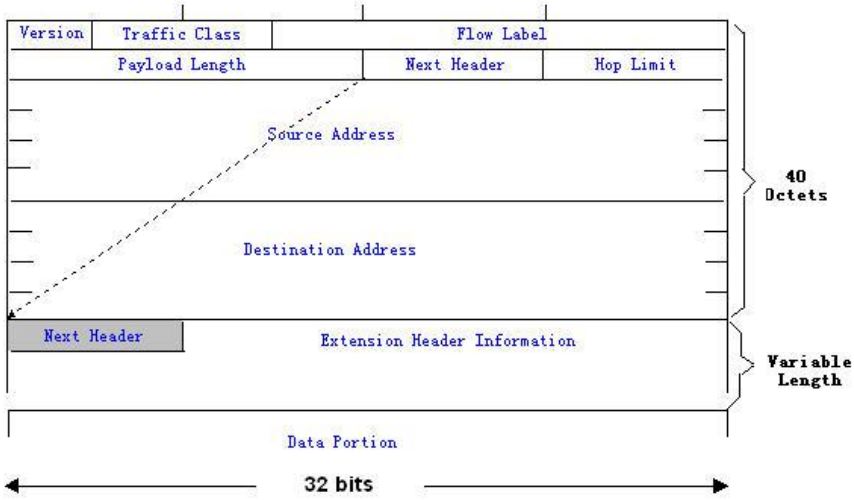
Run the ipv6 address command to configure the IPv6 unicast address and anycast address of an interface.

After an interface goes up, it will automatically join the corresponding multicast group.

1.3.3 IPv6 Packet Header Format

Figure 1-9 shows the format of the IPv6 packet header.

Figure 1-9



The IPv4 packet header is in unit of four bytes. The IPv6 packet header consists of 40 bytes, in unit of eight bytes. The IPv6 packet header has the following fields:

Version

This field consists of 4 bits. In an IPv6 address, this field must be 6.

Traffic Class

This field consists of 8 bits. This field indicates the service provided by this packet, similar to the TOS field in an IPv4 address.

Flow Label

This field consists of 20 bits to identify packets belonging to the same service flow. One node can act as the Tx source of multiple service flows. The flow label and source address uniquely identify one service flow.

Payload Length

This field consists of 16 bits, including the packet payload length and the length of IPv6 extended options (if available). That is, it includes the IPv6 packet length except the IPv6 packet header.

Next Header

This field indicates the protocol type in the header field following the IPv6 packet header. Similar to the Protocol field in the IPv4 address header, the Next Header field is used to indicate whether the upper layer uses TCP or UDP. It can also be used to indicate existence of the IPv6 extension header.

Hop Limit

This field consists of 8 bits. Every time a device forwards a packet, the field value reduced by 1. If the field value reaches 0, this packet will be discarded. It is similar to the Lifetime field in the IPv4 packet header.

Source Address

This field consists of 128 bits and indicates the sender address in an IPv6 packet.

Destination Address

This field consists of 128 bits and indicates the receiver address in an IPv6 packet.

At present, IPv6 defines the following extension headers:

Hop-By-Hop Options

This extension header must follow the IPv6 packet header. It consists of option data to be checked on each node along the path.

Routing Options (Type 0 routing header)

This extension header indicates the nodes that a packet passes through from the source address to the destination address. It consists of the address list of the passerby nodes. The initial destination address in the IPv6 packet header is the first address among the addresses in the routing header, but not the final destination address of the packet. After the node corresponding to the destination address in the IPv6 packet header receives a packet, it processes the IPv6 packet header and routing header, and sends the packet to the second address, the third address, and so on in the routing header list till the packet reaches the final destination address.

Fragment

The source node uses this extension header to fragment the packets of which the length exceeds the path MTU (PMTU).

Destination Options

This extension header replaces the option fields of IPv4. At present, the Destination Options field can only be filled with integral multiples of 64 bits (eight bytes) if required. This extension header can be used to carry information to be checked by the destination node.

Upper-layer header

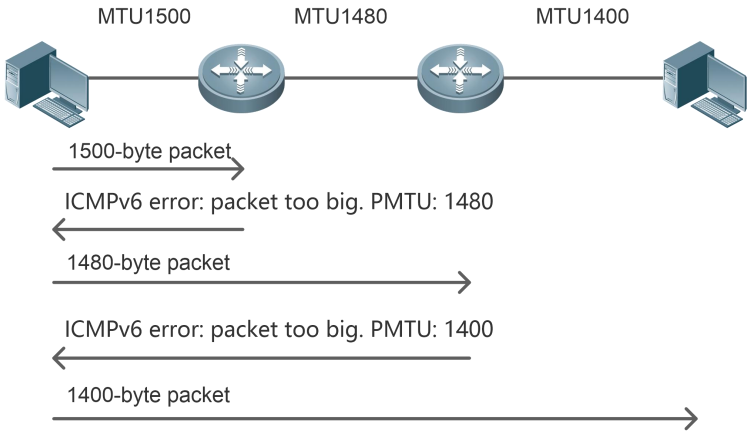
This extension header indicates the protocol used at the upper layer, such as TCP (6) and UDP (17).

Another two extension headers AH and ESP will be described in the *Configuring IPSec*.

1. 3. 4 IPv6 PMTUD

Similar to IPv4 Path MTU Discovery (PMTUD), IPv6 PMTUD allows a host to dynamically discover and adjust the MTU size on the data Tx path. If the length of a data packet to be sent by a host is greater than the PMTU, the host performs packet fragmentation on its own. In this manner, the IPv6 device does not need to perform fragmentation, saving device resources and improving the IPv6 network efficiency.

Figure 1- 10



As shown in Figure 1-10, if the length of a packet to be sent by the host is greater than the PMTU, the router discards this packet and sends an ICMPv6 Packet Too Big message containing its PMTU to the host. The host then fragments the packet based on the new PMTU. In this manner, the router does not need to perform fragmentation, saving router resources and improving the IPv6 network efficiency.

Related Configuration

Configuring the IPv6 MTU of an Interface

The default IPv6 MTU is 1500 on an Ethernet interface.

Run the ipv6 mtu command to modify the IPv6 MTU of an interface.

Configuring the Static PMTU

Run the ipv6 path-mtu command to configure the static PMTU.

Configuring the Aging Time of the Dynamic PMTU

The default aging time is 10 minutes.

Run the ipv6 path-mtu age command to configure the aging time of the dynamic PMTU.

1.3.5 IPv6 Neighbor Discovery

NDP is a basic part of IPv6. Its main functions include router discovery, prefix discovery, parameter discovery, address auto-configuration, address resolution (like ARP), next-hop determination, NUD, DAD, and redirection. NDP defines five ICMP packets: RS (ICMP type: 133), RA (ICMP type: 134), NS (similar to ARP request, ICMP type: 135), NA (similar to ARP reply, ICMP type: 136), ICMP Redirect (ICMP type: 137).

All the above ICMP packets carry one or multiple options. These options are optional in some cases but are significant in other cases. NDP mainly defines five options: Source Link-Layer Address Option, Type=1; Target Link-Layer Address Option, Type=2; Prefix Information Option, Type=3; Redirection Header Option, Type=4; MTU Option, Type=5.

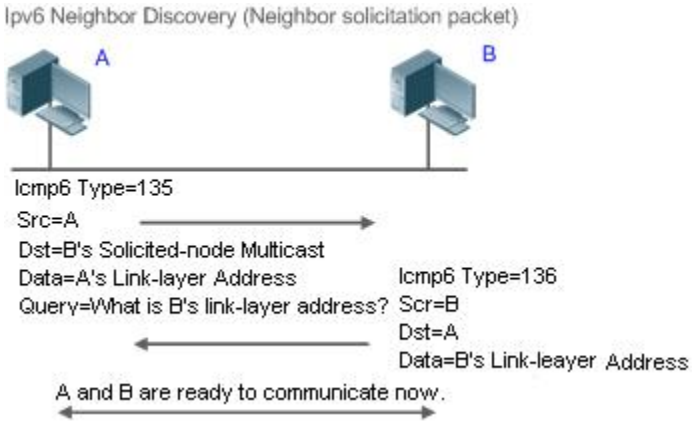
Address Resolution

When a node attempts to communicate with another, the node has to obtain the link-layer address of the peer end by sending it an NS packet. In this packet, the destination address is the solicited-node multicast address corresponding to the IPv6 address of the destination node. This packet also contains the link-layer address of the source node. After receiving this NS packet, the peer end replies

with an NA packet in which the destination address is the source address of the NS packet, that is, the link-layer address of the solicited node. After receiving this NA packet, the source node can communicate with the destination node.

Figure 1- 11 shows the address resolution process.

Figure 1- 11



NUD

If the reachable time of a neighbor has elapsed but an IPv6 unicast packet needs to be sent to it, the device performs NUD.

While performing NUD, the device can continue to forward IPv6 packets to the neighbor.

DAD

To know whether the IPv6 address configured for a host is unique, the device needs to perform DAD by sending an NS packet in which the source IPv6 address is the unspecified address.

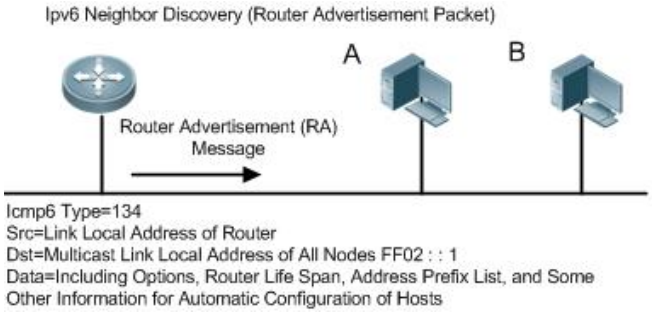
If a device detects an address conflict, this address is set to the duplicate status so that the device cannot receive IPv6 packets with this address being the destination address. Meanwhile, the device also starts a timer for this duplicate address to periodically perform DAD. If no address conflict is detected in re-detection, this address can be properly used.

Router, Prefix, and Parameter Discovery

A device periodically sends RA packets to all local nodes on the link.

Figure 1- 12 shows the RA packet sending process.

Figure 1- 12



An RA packet usually contains the following content:

One or multiple IPv6 address prefixes (used for on-link determination or stateless address auto-configuration)
Validity of the IPv6 address prefix
Host auto-configuration method (stateful or stateless)
Default device information (whether the device acts as the default device; if yes, the interval for acting as the default device is also included.)
Other information provided for host configuration, such as hop limit, MTU, and NS retransmission interval
Routing priority

RA packets can also be used as replies to the RS packets sent by a host. Using RS packets, a host can obtain the auto-configured information immediately after started rather than wait for the RA packets sent by the device. If no unicast address is configured for a newly started host, the host includes the unspecified address (0:0:0:0:0:0:0:0) as the source address in the RS packet. Otherwise, the host uses the configured unicast address as the source address and the multicast address of all local routing devices (FF02::2) as the destination address in the RS packet. As an reply to the RS packet, the RA packet uses the source address of the RS packet as the destination address (if the source address is the unspecified address, it uses the multicast address of all local nodes (FF02::1).

In an RA packet, the following parameters can be configured:

Ra-interval: Interval for sending the RA packet.
Ra-lifetime: Lifetime of a router, that is, whether the device acts as the default router on the local link and the interval for acting as the default router.
Prefix: Prefix of an IPv6 address on the local link. It is used for on-link determination or stateless address auto-configuration, including other parameter configurations related to the prefix.
Ns-interval: NS packet retransmission interval.
Reachabletime: Period when the device regards a neighbor reachable after detecting a Confirm Neighbor Reachability event.
Ra-hoplimit: Hops of the RA packet, used to set the hop limit for a host to send a unicast packet.
Ra-mtu: MTU of the RA packet.
Managed-config-flag: Whether a host receiving this RA packet obtains the address through stateful auto-configuration.
Other-config-flag: Whether a host receiving this RA packet uses DHCPv6 to obtain other information except the IPv6 address for auto-configuration.

Configure the above parameters when configuring IPv6 interface attributes.

The RDNSS and DNSSL options provide IPv6 terminals with the addresses of recursive DNS servers and a search list of DNS domain names.
The URL options offers URLs to IPv6 terminals.

Redirection

If a router receiving an IPv6 packet finds a better next hop, it sends the ICMP Redirect packet to inform the host of the better next hop. The host will directly send the IPv6 packet to the better next hop next time.

Maximum Number of Unresolved ND Entries

You can configure the maximum number of unresolved ND entries to prevent malicious scanning network segments from generating a large number of unresolved ND entries and occupying excessive memory space.

Maximum Number of ND Options

You can configure the maximum number of ND options to prevent forged ND packets from carrying unlimited ND options and occupying excessive CPU space on the device.

Maximum Number of Neighbor Learning Entries on an Interface

You can configure the maximum number of neighbor learning entries on an interface to prevent neighbor learning attacks from occupying ND entries and memory space of the device and affecting forwarding efficiency of the device.

Related Configuration

Enabling IPv6 Redirection

By default, ICMPv6 Redirect packets can be sent on IPv6 interfaces.
Run the no ipv6 redirects command in interface configuration mode to prohibit an interface from sending Redirect packets.

Configuring IPv6 DAD

By default, an interface sends one NS packet to perform IPv6 DAD.
Run the ipv6 nd dad attempts value command in interface configuration mode to configure the number of NS packets consecutively sent by DAD. Value 0 indicates disabling DAD for IPv6 addresses on this interface.
Run the no ipv6 nd dad attempts command to restore the default configuration.
By default, the device performs DAD on duplicate IPv6 addresses every 60 seconds.
Run the ipv6 nd dad retry value command in global configuration mode to configure the DAD interval. Value 0 indicates disabling DAD for the device.
Run the no ipv6 nd dad retry command to restore the default configuration.

Configuring the Reachable Time of a Neighbor

The default reachable time of an IPv6 neighbor is 30s.
Run the ipv6 nd reachable-time milliseconds command in interface configuration mode to modify the reachable time of a neighbor.

Configuring the Stale Time of a Neighbor

The default stale time of an IPv6 neighbor is 1 hour. After the time elapses, the device performs NUD.
Run the ipv6 nd stale-time seconds command in interface configuration mode to modify the stale time of a neighbor.

Configuring Prefix Information

By default, the prefix in an RA packet on an interface is the prefix configured in the ipv6 address command on the interface.
Run the ipv6 nd prefix command in interface configuration mode to add or delete prefixes and prefix parameters that can be advertised.
Run the peer default ipv6 pool command in interface configuration mode to assign a prefix from the prefix pool for advertisement.

Enabling/disabling RA Suppression

By default, an IPv6 interface does not send RA packets.
Run the no ipv6 nd suppress-ra command in interface configuration mode to disable RA suppression.

Configuring the Maximum Number of Unresolved ND Entries

The default value is 0, indicating no restriction. It is only restricted to the ND entry capacity supported by the device.

Run the ipv6 nd unresolved number command in global configuration mode to restrict the number of unresolved neighbors. After the entries exceed this restriction, the device does not actively resolve subsequent packets.

Configuring the Maximum Number of ND Options

Run the ipv6 nd max-opt value command in global configuration mode to restrict the number of ND options to be processed. The default value is 10.

Configuring the Maximum Number of ND Entries Learned on an Interface

Run the ipv6 nd cache interface-limit value command in interface configuration mode to restrict the number of neighbors learned on an interface. The default value is 0, indicating no restriction.

1. 3. 6 Anti-IPv6 ND-DoS Attack

Working Principle

With certain trigger conditions set, anti-IPv6 ND-DoS attack can prevent IPv6 ND entries from being exhausted on the system to ensure proper working of IPv6 ND.

An ND entry refers to the mapping between a MAC address and an IPv6 address, and is used to specify the MAC address corresponding to an IPv6 address. An IPv6 user has only one MAC address but may have multiple IPv6 addresses. That means, a user may correspond to multiple IPv6 ND entries. When an external node sends an NS packet carrying a virtual MAC address to a device, the system generates an ND entry based on the virtual MAC address.

An ND entry has a state maintenance mechanism. A specific state machine is used to promote the aging of ND entries. The aging takes some time, for example, 1 hour. When a host continuously sends an NS packet carrying a virtual MAC address to a device, the device generates corresponding IPv6 ND entries. These entries need time to age, causing the generation faster than the aging. Therefore, when the IPv6 neighboring table becomes full, the device cannot continue proper IPv6 ND, thereby affecting system functions. This is how ND DoS attacks work.

When the ratio of the IPv6 ND entries learned by the system to the maximum number of entries in the IPv6 neighboring table reaches the preset threshold, the anti-IPv6 ND-DoS attack function accelerates the aging of staled ND entries. If the number of IPv6 ND entries corresponding to an MAC address exceeds the preset threshold, this function accelerates the aging of IPv6 ND entries in which this MAC address is in STALE state.

While accelerating the aging of staled IPv6 neighbors, this function can continue to properly learn IPv6 ND entries.

Related Configuration

Configuring the ND Entry Ratio on the Entire System

Run the ipv6 nd threshold percent_value command in global configuration mode.

The default percent_value is 70.

Configuring the Number of ND Entries on a Host

Run the ipv6 nd threshold per-mac value command in global configuration mode.

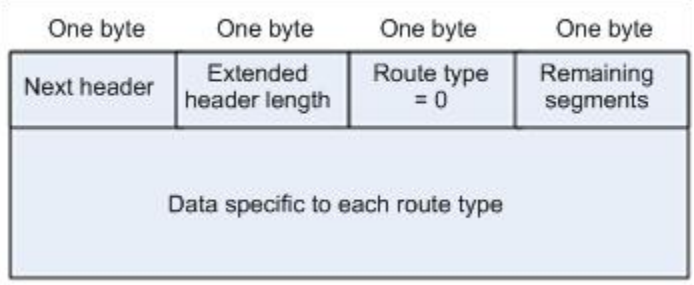
The value ranges from 4 to 256. The default value is 16.

1. 3. 7 IPv6 Source Routing

Working Principle

Similar to the IPv4 loose source routing and loose record routing options, the IPv6 routing header is used to specify the intermediate nodes that the packet passes through along the path to the destination address. It uses the following format:

Figure 1- 13



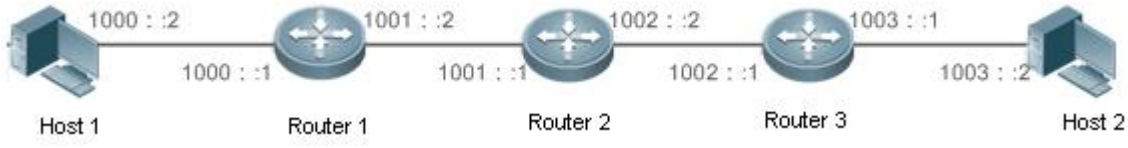
The Segments Left field is used to indicate how many intermediate nodes are specified in the routing header for the packet to pass through from the current node to the final destination address.

Currently, two routing types are defined: 0 and 2. The Type 2 routing header is used for mobile communication. RFC 2460 defines the Type 0 routing header (similar to the loose source routing option of IPv4). The format of the Type 0 routing header is as follows:

Figure 1- 14

The following example describes the application of the Type 0 routing header, as shown in Figure 1- 15.

Figure 1- 15



Host 1 sends Host 2 a packet specifying the intermediate nodes Router 2 and Router 3. The following table lists the changes of fields related to the IPv6 header and routing header during the forwarding process.

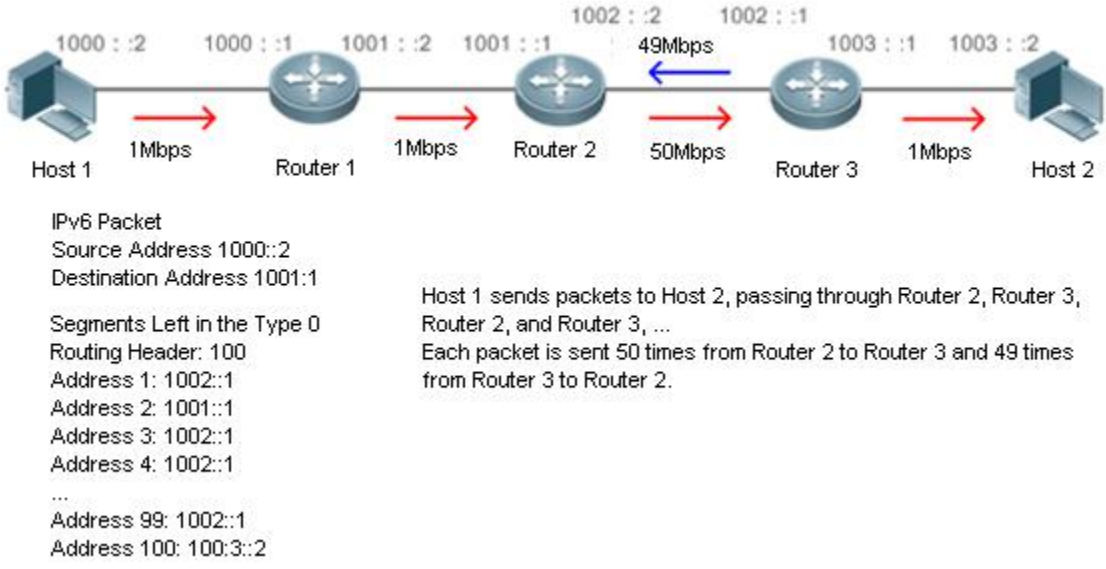
Transmission Node	Fields in the IPv6 Header	Fields Related to the Type 0 Routing Header
Host 1	Source address=1000::2 Destination address=1001::1 (Address of Router 2)	Segments Left=2 Address 1=1002::1 (Address of Router 3) Address 2=1003::2 (Address of Host 2)
Router 1	No change	
Router 2	Source address=1000::2 Destination address=1002::1 (Address of Router 3)	Segments Left=1 Address 1=1001::1 (Address of Router 2) Address 2=1003::2 (Address of Host 2)
Router 3	Source address=1000::2 Destination address=1003::2 (Address of Host 2)	Segments Left=0 Address 1=1001::1 (Address of Router 2) Address 1=1002::2 (Address of Router 3)
Host 2	No change	

The forwarding process is as follows:

1. Host 1 sends a packet in which the destination address is Router 2's address 1001::1, the Type 0 routing header is filled with Router 3's address 1002::1 and Host 2's address 1003::2, and the value of the Segments Left field is 2.
2. Router 1 forwards this packet to Router 2.
3. Router 2 changes the destination address in the IPv6 header to Address 1 in the routing header. That is, the destination address becomes Router 3's address 1002::1, Address 1 in the routing header becomes Router 2's address 1001::1, and the value of the Segments Left field becomes 1. After modification, Router 2 forwards the packet to Router 3.
4. Router 3 changes the destination address in the IPv6 header to Address 2 in the routing header. That is, the destination address becomes Host 2's address 1003::2, Address 2 in the routing header becomes Router 3's address 1002::1, and the value of the Segments Left field becomes 0. After modification, Router 3 forwards the packet to Host 2.

The Type 0 routing header may be used to initiate DoS attacks. As shown in Figure 1- 16, Host 1 sends packets to Host 2 at 1 Mbps and forges a routing header to cause multiple round-trips between Router 2 and Router 3 (50 times from Router 2 to Router 3 and 49 times from Router 3 to Router 2). At the time, the routing header generates the traffic amplification effect:" 50 Mbps from Router 2 to Router 3 and 49 Mbps from Router 3 to Router 2." Due to this security problem, RFC 5095 abolished the Type 0 routing header.

Figure 1- 16



Related Configuration

Enabling IPv6 Source Routing

The Type 0 routing header is not supported by default.

Run the ipv6 source-route command in global configuration mode to enable IPv6 source routing.

1. 3. 8 Restricting the Sending Rate of ICMPv6 Error Messages

Working Principle

The destination node or intermediate router sends ICMPv6 error messages to report the errors incurred during IPv6 data packet forwarding and transmission. There are mainly four types of error messages: Destination Unreachable, Packet Too Big, Time Exceeded, and Parameter Problem.

When receiving an invalid IPv6 packet, a device discards the packet and sends back an ICMPv6 error message to the source IPv6 address. In the case of invalid IPv6 packet attacks, the device may continuously reply to ICMPv6 error messages till device resources are exhausted and thereby fail to properly provide services. To solve this problem, you can restrict the sending rate of ICMPv6 error messages.

If the length of an IPv6 packet to be forwarded exceeds the IPv6 MTU of the outbound interface, the router discards this IPv6 packet and sends back an ICMPv6 Packet Too Big message to the source IPv6 address. This error message is mainly used as part of the IPv6 PMTUD process. If the sending rate of ICMPv6 error messages is restricted due to excessive other ICMPv6 error messages, ICMPv6 Packet Too Big messages may be filtered, causing failure of IPv6 PMTUD. Therefore, it is recommended to restrict the sending rate of ICMPv6 Packet Too Big messages independently of other ICMPv6 error messages.

Although ICMPv6 Redirect packets are not ICMPv6 error messages, FS recommends restricting their rates together with ICMPv6 error messages except Packet Too Big messages.

Related Configuration

Configuring the Sending Rate of ICMPv6 Packet Too Big Messages

The default rate is 10 per 100 ms.

Run the ipv6 icmp error-interval too-big command to configure the sending rate of ICMPv6 Packet Too Big messages.

Configuring the Sending Rate of Other ICMPv6 Error Messages

The default rate is 10 per 100 ms.
Run the ipv6 icmp error-interval command to configure the sending rate of other ICMPv6 error messages.

1.3.9 IPv6 Hop Limit

Working Principle

An IPv6 data packet passes through routers from the source address and destination address. If a hop limit is configured, it decreases by one every time the packet passes through a router. When the hop limit decreases to 0, the router discards the packet to prevent this useless packet from being unlimitedly transmitted on the network and wasting network bandwidth. The hop limit is similar to the TTL of IPv4.

Related Configuration

Configuring the IPv6 Hop Limit

The default IPv6 hop limit of a device is 64.
Run the ipv6 hop-limit command to configure the IPv6 hop limit of a device.

1.3.10 Refraining from Sending NS Packets to Authentication VLANs

Working Principle

In gateway authentication mode, all sub VLANs in a super VLAN are authentication VLANs by default. Users in an authentication VLAN have to pass authentication to access the network. After authentication, a static ND entry is generated on the device. Therefore, when accessing an authenticated user, the device does not need to send NS packets to the authentication VLAN. If the device attempts to access users in an authentication-free VLAN, it only needs to send NS requests to the authentication-free VLAN.

In gateway authentication mode, the function of refraining from sending NS packets to authentication VLANs is enabled on the device by default. If the device needs to access authentication-free users in an authentication VLAN, disable this function.

Related Configuration

Enabling the Function of Refraining from Sending NS Packets to Authentication VLANs

Run the ipv6 nd suppress-auth-vlan-ns command in interface configuration mode to enable the function of refraining from sending NS packets to authentication VLANs.
This function is enabled by default.
This function is supported only on switch virtual interfaces (SVIs) and takes effect only in gateway authentication mode.

1.3.11 Default Gateway on the Management Interface

Working Principle

The default gateway is configured on the management interface to generate a default route for this interface.

Related Configuration

Configuring the Default Gateway on the Management Interface

Run the ipv6 gateway ipv6-address command in interface configuration mode to configure the default gateway on the management interface.

No default gateway is configured on the management interface by default.

1.3.12 Assigning Different IPv6 Prefixes to Different Users

Working Principle

A specified prefix pool is configured on an interface to assign different IPv6 prefixes to different users bound to the interface.

Related Configuration

Configuring the Prefix on an Interface

Run the ipv6 local pool pool-name ipv6-prefix/prefix-length prefix-length command in global configuration mode to assign a prefix pool.

Run the ipv6 nd prefix pool pool-name command in interface configuration mode to configure the name of the prefix pool bound to the interface.

1.4 Configuration

Configuration	Description and Command	
Configuring an IPv6 Address	(Mandatory) It is used to configure IPv6 addresses and enable IPv6.	
	ipv6 enable	Enables IPv6 on an interface.
	ipv6 address	Configures the IPv6 unicast address of an interface.
	(Optional) It is used to borrow an IP address from another interface.	
	ipv6 unnumbered	Configures an interface to borrow the unicast address of another interface.
Configuring IPv6 NDP	(Optional) It is used to enable IPv6 redirection on an interface.	
	ipv6 redirects	Enables IPv6 redirection on an interface.
	(Optional) It is used to enable DAD.	
	ipv6 nd dad attempts	Configures the number of consecutive NS packets sent during DAD.
	(Optional) It is used to configure ND parameters.	
	ipv6 nd reachable-time	Configures the reachable time of a neighbor.
	ipv6 nd prefix	Configures the address prefix to be advertised in an RA packet.
	peer default ipv6 pool	Configures an RA packet to obtain the prefix from the prefix pool.
	ipv6 nd suppress-ra	Enables RA suppression on an interface.

Configuration	Description and Command	
	(Optional) It is used to configure the maximum number of unresolved ND entries.	
	ipv6 nd unresolved	Configures the maximum number of unresolved ND entries.
	(Optional) It is used to configure the maximum number of ND options.	
	ipv6 nd max-opt	Configures the maximum number of ND options.
	(Optional) It is used to configure the maximum number of neighbors learned on an interface.	
	ipv6 nd cache interface-limit	Configures the maximum number of neighbors learned on an interface.
Enabling Anti-IPv6 ND-DoS Attack	(Optional) It is used to configure the ND entry ratio on the entire system.	
	ipv6 nd threshold	Configures the ND entry ratio on the entire system.
	(Optional) It is used to configure the number of ND entries on a host.	
	ipv6 nd threshold per-mac	Configures the number of ND entries on a host.
Enabling PMTUD	(Optional) It is used to restrict the MTU of IPv6 packets sent on an interface.	
	ipv6 mtu	Configures the IPv6 MTU.
Enabling IPv6 Source Routing	(Optional) It is used to enable IPv6 source routing.	
	ipv6 source-route	Configures the device to forward IPv6 packets carrying the routing header.
Configuring the Sending Rate of ICMPv6 Error Messages	Optional.	
	ipv6 icmp error-interval too-big	Configures the sending rate of ICMPv6 Packet Too Big messages.
	ipv6 icmp error-interval	Configures the sending rates of other ICMPv6 error messages and ICMPv6 Redirect packets.
Configuring the IPv6 Hop Limit	(Optional) It is used to restrict the hop limit of IPv6 unicast packets sent on an interface.	
	ipv6 hop-limit	Configures the IPv6 hop limit.
Enabling Refraining from Sending NS Packets to Authentication VLANs	(Optional) It is used to restrict sending NS packets to authentication VLANs in gateway authentication mode.	
	ipv6 nd suppress-auth-vlan-ns	Enables NS broadcast suppression in authentication VLANs.
Configuring the Default Gateway on the Management Interface	(Optional) It is used to configure the default gateway on the management interface.	
	ipv6 gateway *ipv6-address*	Configures the default gateway on the management interface.
Assigning Different IPv6 Prefixes to Different Users	(Optional) It is used to configure the default gateway on the management interface.	
	ipv6 nd prefix pool *pool-name*	Configures an IPv6 prefix pool on an interface.

1.4.1 Configuring an IPv6 Address

Configuration Effect

Configure the IPv6 address of an interface to implement IPv6 network communication.

Configuration Steps

Enabling IPv6 on an Interface

(Optional) If you do not want to enable IPv6 by configuring an IPv6 address, run the ipv6 enable command.

Configuring the IPv6 Unicast Address of an Interface

Mandatory.

Configuring an Interface to Borrow the Unicast Address of Another Interface

Run the ipv6 unnumbered command to configure an interface to borrow an IPv6 address.
(Optional) This command is supported only on Point to Point Protocol (PPP) interfaces.

Verification

Run the **show ipv6 interface** command to check whether the configured address takes effect.

Related Commands

Enabling IPv6 on an Interface

Command	**ipv6 enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	IPv6 can be enabled on an interface by two methods: 1) running the **ipv6 enable** command in interface configuration mode; 2) configuring an IPv6 address on the interface. If an interface is bound to a multiprotocol VRF instance configured with no IPv6 address family, IPv6 cannot be enabled on this interface. You can enable IPv6 on this interface only after configuring an IPv6 address family for the multiprotocol VRF. If an IPv6 address is configured on an interface, IPv6 is automatically enabled on this interface. In this case, IPv6 cannot be disabled even when you run the **no ipv6 enable** command.

Configuring the IPv6 Unicast Address of an Interface

Command	**ipv6 address** *ipv6-address* / *prefix-length* **ipv6 address** *ipv6-prefix* / *prefix-length* **eui-64** **ipv6 address** *prefix-name sub-bits* / *prefix-length* [**eui-64**]

Parameter Description	*ipv6-address*: Indicates the IPv6 address, which must comply with the address format defined in RFC 4291. Separated by a colon (:), each address field consists of 16 bits and is represented by hexadecimal digits. *ipv6-prefix*: Indicates the IPv6 address prefix, which must comply with the address format defined in RFC 4291. *prefix-length*: Indicates the length of the IPv6 address prefix, that is, the part representing the network in the IPv6 address. *prefix-name*: Indicates the name of the universal prefix. This specified universal prefix is used to create the interface address. *sub-bits*: Indicates the subprefix bits and host bits of the address to be concatenated with the prefixes provided by the general prefix specified with the *prefix-name* parameter. This value is combined with the universal prefix to create the interface address. This value must be in the form documented in RFC 4291. *eui-64*: Indicates the created IPv6 address, consisting of the configured address prefix and 64-bit interface ID.
Command Mode	Interface configuration mode
Usage Guide	If an interface is bound to a multiprotocol VRF instance configured with no IPv6 address family, the IPv6 address cannot be configured for this interface. You can configure the IPv6 address of this interface only after configuring an IPv6 address family for the multiprotocol VRF. If an IPv6 interface is created and is Up state, the system automatically generates a link-local address for this interface. The IPv6 address of an interface can also be created by the universal prefix mechanism. That is, IPv6 address = Universal prefix + Sub prefix + Host bits. The universal prefix can be configured by running the **ipv6 general-prefix** command or learned by the prefix discovery function of the DHCPv6 client (see the *Configuring DHCPv6*). Sub prefix + Host bits are specified by the *sub-bits* and *prefix-length* parameters in the **ipv6 address** command. If you run the **no ipv6 address** command without specifying an address, all manually configured addresses will be deleted. Run the **no ipv6 address** *ipv6-prefix/prefix-length* **eui-64** command to delete the configured address.

Configuring an Interface to Borrow the Unicast Address of Another Interface

Command	**ipv6 unnumbered** *interface-id*
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	IPv6 unnumbered can save IPv6 addresses and supports only PPP interfaces. If an interface is bound to a multiprotocol VRF instance configured with no IPv6 address family, IPv6 unnumbered cannot be enabled on this interface. You can enable IPv6 unnumbered on this interface only after configuring an IPv6 address family for the multiprotocol VRF. If IPv6 unnumbered is enabled on an interface, IPv6 is automatically enabled on this interface. In this case, IPv6 cannot be disabled even when you run the **no ipv6 enable** command.

Configuration Example

Configuring an IPv6 Address on an Interface

Configuration Steps	Enable IPv6 on the GigabitEthernet 0/0 interface and add IPv6 address 2000::1 to the interface.
	FS(config)#interface gigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)#ipv6 enable FS(config-if-GigabitEthernet 0/0)#ipv6 address 2000::1/64
Verification	Run the **show ipv6 interface** command to verify that an address is successfully added to the GigabitEthernet 0/0 interface.
	FS(config-if-GigabitEthernet 0/0)#show ipv6 interface gigabitEthernet 0/0 interface GigabitEthernet 0/0 is Down, ifindex: 1, vrf_id 0 address(es): Mac Address: 00:00:00:00:00:00 INET6: FE80::200:FF:FE00:1 [TENTATIVE], subnet is FE80::/64 INET6: 2000::1 [TENTATIVE], subnet is 2000::/64 Joined group address(es): MTU is 1500 bytes ICMP error messages limited to one every 100 milliseconds ICMP redirects are enabled ND DAD is enabled, number of DAD attempts: 1 ND reachable time is 30000 milliseconds ND advertised reachable time is 0 milliseconds ND retransmit interval is 1000 milliseconds ND advertised retransmit interval is 0 milliseconds ND router advertisements are sent every 200 seconds<160--240> ND router advertisements live for 1800 seconds

1.4.2 Configuring IPv6 NDP

Configuration Effect

Configure NDP-related attributes, for example, enable IPv6 redirection and DAD.

Notes

RA suppression is enabled on interfaces by default. To configure a device to send RA packets, run the **no ipv6 nd suppress-ra** command in interface configuration mode.

Configuration Steps

Enabling IPv6 Redirection on an Interface

(Optional) IPv6 redirection is enabled by default.

To disable IPv6 redirection on an interface, run the no ipv6 redirects command.

Configuring the Number of Consecutive NS Packets Sent During DAD

Optional.

To prevent enabling DAD for IPv6 addresses on an interface or modify the number of consecutive NS packets sent during DAD, run the ipv6 nd dad attempts command.

Configuring the Reachable Time of a Neighbor

Optional.

To modify the reachable time of a neighbor, run the ipv6 nd reachable-time command.

Configuring the Address Prefix to Be Advertised in an RA Packet

By default, the prefix in an RA packet on an interface is the prefix configured in the ipv6 address command on the interface.

(Optional) Run the ipv6 nd prefix command to add or delete prefixes and prefix parameters that can be advertised. Or run the peer default ipv6 pool command to assign a prefix from the prefix pool for advertisement

Enabling/Disabling RA Suppression on an Interface

Optional.

If a device needs to send RA packets, run the no ipv6 nd suppress-ra command.

Configuring the Maximum Number of Unresolved ND Entries

Optional.

If a large number of unresolved ND entries are generated due to scanning attacks, run the ipv6 nd unresolved command to restrict the number of unresolved neighbors.

Configuring the Maximum Number of ND Options

Optional.

If a device needs to process more options, run the ipv6 nd max-opt command.

Configuring the Maximum Number of ND Entries Learned on an Interface

Optional.

If the number of IPv6 hosts is controllable, run the ipv6 nd cache interface-limit command to restrict the number of neighbors learned on an interface. This prevents ND learning attacks from occupying the memory space and affecting device performance.

Verification

Run the following commands to check whether the configuration is correct:

show ipv6 interface interface-type interface-num: Check whether the configurations such as the redirection function, reachable time of a neighbor, and NS sending interval take effect.
show ipv6 interface interface-type interface-num ra-inifo: Check whether the prefix and other information configured for RA packets are correct.
show run

Related Commands

Enabling IPv6 Redirection on an Interface

Command	**ipv6 redirects**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	All ICMPv6 error messages are transmitted at a limited transmission rate. By default, a maximum number of 10 ICMPv6 error messages are transmitted per second (10 pps).

Configuring the Number of Consecutive NS Packets Sent During DAD

Command	**ipv6 nd dad attempts** *value*
Parameter Description	*value*: Indicates the number of NS packets.
Command Mode	Interface configuration mode
Usage Guide	You need to enable DAD before configuring an IPv6 address on an interface. Then the address is in tentative state. If no address conflict is detected by DAD, this address can be correctly used. If an address conflict is detected and the interface ID of this address uses EUI-64, duplicate link-layer addresses exist on this link. In this case, the system automatically disables this interface to prevent IPv6-related operations on this interface). At the time, you must configure a new address and restart the interface to re-enable DAD. When an interface changes from the down state to the up state, DAD is re-enabled for the addresses on this interface.

Configuring the Reachable Time of a Neighbor

Command	**ipv6 nd reachable-time** *milliseconds*
Parameter Description	*milliseconds*: Indicates the reachable time of a neighbor, ranging from 0 to 3,600,000. The unit is millisecond. The default value is 30s.
Command Mode	Interface configuration mode
Usage Guide	A device detects unreachable neighbors based on the configured reachable time. The shorter the configured reachable time, the faster the device detects unreachable neighbors but the more it consumes network bandwidth and device resources. Therefore, it is not recommended to set this time too small. The configured value is advertised in an RA packet and is also used on the device. If the value is 0, the reachable time

	is not specified on the device and it is recommended to use the default value.

Configuring the Address Prefix to Be Advertised in an RA Packet

Command	**ipv6 nd prefix** {*ipv6-prefix*/*prefix-length* | **default**} [[*valid-lifetime* { **infinite** / *preferred-lifetime* }] | [**at** *valid-date preferred-date*] | [**infinite** {**infinite** | *preferred-lifetime*}]] [**no-advertise**] | [[**off-link**] [**no-autoconfig**]]
Parameter Description	*ipv6-prefix*: Indicates the network ID of IPv6, which must comply with the address representation format in RFC 4291. *prefix-length*: Indicates the length of the IPv6 address prefix. A slash (/) must be added before the prefix. *valid-lifetime*: Indicates the period when a host receiving the prefix of an RA packet regards the prefix valid. The value ranges from 0 to 4,294,967,295. The default value is 30 days. *preferred-lifetime*: Indicates the preferred period when a host receiving the prefix of an RA packet regards the prefix valid. The value ranges from 0 to 4,294,967,295. The default value is 7 days. **at** *valid-date preferred-date*: Indicates the valid date and preferred deadline configured for the RA prefix. It uses the format of *dd+mm+yyyy+hh+mm*. **infinite**: Indicates that the prefix is permanently valid. **default**: Indicates that the default parameter configuration is used. **no-advertise**: Indicates that the prefix is not advertised by a router. **off-link**: If the prefix of the destination address in the IPv6 packet sent by a host matches the configured prefix, the device regards the destination address on the same link and directly reachable. This parameter indicates that this prefix does not require on-link determination. **no-autoconfig**: Indicates that the prefix in the RA packet received by a host cannot be used for address auto-configuration.
Command Mode	Interface configuration mode
Usage Guide	This command can be used to configure parameters related to each prefix, including whether to advertise this prefix. By default, an RA packet uses the prefix configured by running the **ipv6 address** command. Run the **ipv6 nd prefix** command to add other prefixes. Run the **ipv6 nd prefix default** command to configure the default parameters for an interface. That is, if no parameter is specified when a prefix is added, use the parameters configured in the **ipv6 nd prefix default** command as the parameters of the new prefix. The default parameter configurations are abandoned once a parameter is specified for the prefix. That is, when you use the **ipv6 nd prefix default** command to modify the default parameter configurations, only the prefix configured for the default parameters changes and configurations of the prefix remain the same. **at** *valid-date preferred-date*: You can specify the valid date of the prefix in two methods: 1) specifying a fixed time for each prefix in an RA packet; 2) specifying the deadline. In the second method, the valid date of the prefix in each RA packet decreases till it becomes 0.

Enabling/Disabling RA Suppression on an Interface

Command	**ipv6 nd suppress-ra**
Parameter Description	N/A
Command Mode	Interface configuration mode

Usage Guide	To enable RA suppression on an interface, run the **ipv6 suppress-ra** command.

Configuring the Maximum Number of Unresolved ND Entries

Command	**ipv6 nd unresolved** *number*
Parameter Description	*number*: Indicates the maximum number of unresolved ND entries.
Command Mode	Global configuration mode
Usage Guide	To prevent malicious scanning attacks from creating a large number of unresolved ND entries and occupying entry resources, you can restrict the number of unresolved ND entries.

Configuring the Maximum Number of ND Options

Command	**ipv6 nd max-opt** *value*
Parameter Description	*value*: Indicates the number of supported ND options.
Command Mode	Global configuration mode
Usage Guide	Configure the maximum number of ND options processed by a device, such as link-layer address option, MTU option, redirection option, and prefix option.

Configuring the Maximum Number of ND Entries Learned on an Interface

Command	**ipv6 nd cache interface-limit** *value*
Parameter Description	*value*: Indicates the maximum number of neighbors learned by an interface.
Command Mode	Interface configuration mode
Usage Guide	Restricting the number of ND entries learned on an interface can prevent malicious neighbor attacks. If this number is not restricted, a large number of ND entries will be generated on the device, occupying excessive memory space. The configured value must be equal to or greater than the number of the ND entries learned by the interface. Otherwise, the configuration does not take effect. The configuration is subject to the ND entry capacity supported by the device.

Configuration Example

Enabling IPv6 Redirection on an Interface

Configuration Steps	Enable IPv6 redirection on interface GigabitEthernet 0/0.
	FS(config-if-GigabitEthernet 0/0)#ipv6 redirects
Verification	Run the **show ipv6 interface** command to check whether the configuration takes effect.

Configuration Steps	Enable IPv6 redirection on interface GigabitEthernet 0/0.
	FS(config-if-GigabitEthernet 0/0)#ipv6 redirects
Verification	Run the **show ipv6 interface** command to check whether the configuration takes effect.
	FS#show ipv6 interface gigabitEthernet 0/0 interface GigabitEthernet 0/0 is Down, ifindex: 1, vrf_id 0 address(es): Mac Address: 00:00:00:00:00:00 INET6: FE80::200:FF:FE00:1 [TENTATIVE], subnet is FE80::/64 Joined group address(es): MTU is 1500 bytes ICMP error messages limited to one every 100 milliseconds ICMP redirects are enabled ND DAD is enabled, number of DAD attempts: 1 ND reachable time is 30000 milliseconds ND advertised reachable time is 0 milliseconds ND retransmit interval is 1000 milliseconds ND advertised retransmit interval is 0 milliseconds ND router advertisements are sent every 200 seconds<160--240> ND router advertisements live for 1800 seconds

Configuring IPv6 DAD

Configuration Steps	Configure the interface to send three consecutive NS packets during DAD.
	FS(config-if-GigabitEthernet 0/0)# ipv6 nd dad attempts 3
Verification	Run the **show ipv6 interface** command to check whether the configuration takes effect.
	FS#show ipv6 interface gigabitEthernet 0/0 interface GigabitEthernet 0/0 is Down, ifindex: 1, vrf_id 0 address(es): Mac Address: 00:00:00:00:00:00 INET6: FE80::200:FF:FE00:1 [TENTATIVE], subnet is FE80::/64

	Joined group address(es): MTU is 1500 bytes ICMP error messages limited to one every 100 milliseconds ICMP redirects are enabled ND DAD is enabled, number of DAD attempts: 3 ND reachable time is 30000 milliseconds ND advertised reachable time is 0 milliseconds ND retransmit interval is 1000 milliseconds ND advertised retransmit interval is 0 milliseconds ND router advertisements are sent every 200 seconds<160--240> ND router advertisements live for 1800 seconds FS(config-if-GigabitEthernet 0/0)#

Configuring Prefix Information in an RA Packet

Configuration Steps	Add a prefix 1234::/64 to interface GigabitEthernet 0/0.
	FS(config-if-GigabitEthernet 0/0)#ipv6 nd prefix 1234::/6
Verification	Run the **show ipv6 interface** command to check whether the configuration takes effect.
	FS#show ipv6 interface gigabitEthernet 0/0 ra-info GigabitEthernet 0/0: DOWN (RA is suppressed) RA timer is stopped waits: 0, initcount: 0 statistics: RA(out/in/inconsistent): 0/0/0, RS(input): 0 Link-layer address: 00:00:00:00:00:00 Physical MTU: 1500 ND router advertisements live for 1800 seconds ND router advertisements are sent every 200 seconds<160--240> Flags: !M!O, Adv MTU: 1500 ND advertised reachable time is 0 milliseconds ND advertised retransmit time is 0 milliseconds ND advertised CurHopLimit is 64 Prefixes: <total: 1>

Configuration Steps	Add a prefix 1234::/64 to interface GigabitEthernet 0/0.
	FS(config-if-GigabitEthernet 0/0)#ipv6 nd prefix 1234::/6
Verification	Run the **show ipv6 interface** command to check whether the configuration takes effect.
	1234::/64(Def, CFG, vltime: 2592000, pltime: 604800, flags: LA)

Configuring RA Packets to Obtain Prefixes from the Prefix Pool

Configuration Steps	Configure RA packets to obtain prefixes from the prefix pool "ra-pool".
	FS(config-if-GigabitEthernet 0/0)#peel default ipv6 pool ra-pool
Verification	Run the **show run** command to check whether the configuration takes effect.

	FS(config-if-GigabitEthernet 0/0)#show run interface gigabitEthernet 0/0
	
	Building configuration...
	Current configuration : 125 bytes
	
	interface GigabitEthernet 0/0
	  ipv6 enable
	  no ipv6 nd suppress-ra
	peel default ipv6 pool ra-pool
	!

Disabling RA Suppression

Configuration Steps	Disable RA suppression on an interface.
	FS(config-if-GigabitEthernet 0/0)# no ipv6 nd suppress-ra
Verification	Run the **show run** command to check whether the configuration takes effect.
	FS(config-if-GigabitEthernet 0/0)#show run interface gigabitEthernet 0/0 Building configuration... Current configuration : 125 bytes interface GigabitEthernet 0/0

Configuration Steps	Disable RA suppression on an interface.
	FS(config-if-GigabitEthernet 0/0)# no ipv6 nd suppress-ra
Verification	Run the **show run** command to check whether the configuration takes effect.
	ipv6 enable no ipv6 nd suppress-ra !

Configuring the Maximum Number of Unresolved ND Entries

Configuration Steps	Set the maximum number of unresolved ND entries to 200.
	FS(config)# ipv6 nd unresolved 200
Verification	Run the **show run** command to check whether the configuration takes effect.
	FS#show run ipv6 nd unresolved 200 !

Configuring the Maximum Number of ND Options

Configuration Steps	Set the maximum number of ND options to 20.
	FS(config)# ipv6 nd max-opt 20
Verification	Run the **show run** command to check whether the configuration takes effect.
	FS#show run ipv6 nd max-opt 20 !

Configuring the Maximum Number of ND Entries Learned on an Interface

Configuration Steps	Set the maximum number of ND entries learned on an interface to 100.
	FS(config-if-GigabitEthernet 0/1)# ipv6 nd cache interface-limit 100
Verification	Run the **show run** command to check whether the configuration takes effect.

Configuration Steps	Set the maximum number of ND entries learned on an interface to 100.
	FS(config-if-GigabitEthernet 0/1)# ipv6 nd cache interface-limit 100
Verification	Run the **show run** command to check whether the configuration takes effect.
	FS#show run ! interface GigabitEthernet 0/1 ipv6 nd cache interface-limit 100 !

1.4.3 Enabling Anti-IPv6 ND-DoS Attack

Configuration Effect

Enable anti-IPv6 ND-DoS attack on a device.

Configuration Steps

Configuring the ND Entry Ratio on the Entire System

Optional.

Configuring the Number of ND Entries on a Host

Optional.

Verification

Run the show running-config command to check whether the configuration is correct.

Related Commands

Configuring the ND Entry Ratio on the Entire System

Command	**ipv6 nd threshold** *percent_value*
Parameter Description	*percent_value*: If the ratio of the ND entry quantity to the ND entry capacity exceeds this value, anti-IPv6 ND-DoS attack is enabled.
Command Mode	Global configuration mode
Usage Guide	*percent_value* indicates the ratio of the current ND entry quantity to the ND entry capacity supported by the device. If the IPv6 ND entry ratio reaches the threshold configured in this command, the device performs NUD on staled ND entries. However, ND is not affected, and therefore the device can continue to learn new ND entries.

Configuring the Number of ND Entries on a Host

Command	**ipv6 nd threshold per-mac** *value*
Parameter Description	*value:* If the number of IPv6 ND entries on a host exceeds this value, anti-IPv6 ND-DoS attack is enabled on the host.
Command Mode	Global configuration mode
Usage Guide	This command is used to enable ND anti-DoS attack for a host. When the IPv6 ND entries corresponding to a host reaches the value specified by this command, the device performs NUD on the staled IPv6 ND entries of the host. Other hosts are not affected if the numbers of their IPv6 ND entries do not reach this value. ND is not affected, and therefore the device can continue to learn new ND entries.

Configuration Example

Configuring the ND Entry Ratio on the Entire System

Configuration Steps	Set the ND entry capacity ratio on the entire system to 80% to enable ND anti-DoS attack.
	FS(config)# ipv6 nd threshold 80
Verification	Run the **show running-config** command to check whether the configuration takes effect.

Configuring the Number of ND Entries on a Host

Configuration Steps	Set the number of ND entries on a host to 100 to enable ND anti-DoS attack.
	FS(config)# ipv6 nd threshold per-mac 100
Verification	Run the **show running-config** command to check whether the configuration takes effect.

1.4.4 Enabling PMTUD

Configuration Effect

When sending an IPv6 packet, a host fragments the packet based on the PMTU.

Notes

The IPv6 MTU of an interface must be less than or equal to the interface MTU.

Configuration Steps

Configuring the IPv6 MTU of an Interface

Optional.

Configuring the Static PMTU

Optional.

Configuring the Aging Time of the Dynamic PMTU

Optional.

Verification

Run the show run command to check whether the configuration is correct.
Run the show ipv6 interface command to check whether the IPv6 MTU of an interface is correct.
Run the show ipv6 path-mtu command to display the PMTU.
Capture the locally sent IPv6 packets of which the length exceeds the PMTU. The packet capture result shows that the IPv6 packet is fragmented based on the PMTU.

Related Commands

Configuring the IPv6 MTU of an Interface

Command	**ipv6 mtu** *bytes*
Parameter Description	*bytes*: Indicates the MTU of an IPv6 packet, ranging from 1280 to 1500. The unit is byte.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the Static PMTU

Command	**ipv6 path-mtu** [**vrf** *vrf-name*] *ipv6-address value* **ipv6 path-mtu** *ipv6-address value*
Parameter Description	**vrf** *vrf-name*: Indicates the name of a VRF instance. If this parameter is not specified, it indicates the public network. *ipv6-address*: Indicates an IPv6 address, which can be a unicast or multicast address. *value*: Indicates the PMTU, ranging from 1280 to 65,575. The unit is byte.
Command Mode	Global configuration mode
Usage Guide	When sending an IPv6 packet, a host determines which one of the IPv6 MTU and PMTU of the outbound interface is smaller. If the packet length is greater than the smaller MTU, the host fragments the packet based on the smaller MTU. An IPv6 multicast packet may pass through multiple paths to different nodes. Therefore, the PMTU of the multicast address uses the minimum value among the PMTUs of all paths. If the VRF instance name and IPv6 address are the same, static PMTUs overwrite dynamic PMTUs while dynamic PMTUs cannot overwrite static PMTUs. Run the **no ipv6 path-mtu all** command to delete all static PMTUs. Run the **show ipv6 path-mtu statistics** command to display the capacity and current number of static PMTUs.

Configuring the Aging Time of the Dynamic PMTU

Command	**ipv6 path-mtu age** { *age-time* / **infinity** }
Parameter Description	*age-time*: Indicates the aging time in unit of minute. The value ranges from 10 to 43,200 (30 x 24 x 60). The default value is 10 minutes. **infinity**: Indicates that the aging time is infinitely large, that is, the PMTU never ages.
Command Mode	Global configuration mode
Usage Guide	Before aging, dynamic PMTUs can only decrease. Since the network topology and route may change in actual situations, the path also changes and the learned PMTU is less than the actual PMTU. Therefore, the node needs to periodically age the PMTU and relearn the PMTU. When the aging time of dynamic PMTUs elapses, the device deletes the dynamic PMTUs. Before the PMTU is relearned, long IPv6 packets may be discarded by the router during forwarding. When the LAN connects to the Internet through a link with a small MTU, you can determine that this MTU is the smallest among all paths. In this case, you should increase the aging time or configure an infinite aging time to prevent packet drops every 10 minutes.

Configuration Example

Configuring the IPv6 MTU of an Interface

Configuration Steps	Change the IPv6 MTU of interface GigabitEthernet 0/0 to 1,300.
	FS(config-if-GigabitEthernet 0/0)#ipv6 mtu 1300
Verification	Run the **show ipv6 interface** command to check whether the configuration takes effect.

	FS(config-if-GigabitEthernet 0/0)#show ipv6 interface
	
	interface GigabitEthernet 0/ is Down, ifindex: 1, vrf_id 0
	  address(es):
	  Mac Address: 00:d0:f8:22:33:47
	  INET6: FE80::2D0:F8FF:FE22:3347 [TENTATIVE], subnet is FE80::/64
	  INET6: 1020::1 [TENTATIVE], subnet is 1020::/64
	  INET6: 1023::1 [TENTATIVE], subnet is 1023::/64
	  Joined group address(es):
	  MTU is 1300 bytes
	  ICMP error messages limited to one every 100 milliseconds
	  ICMP redirects are enabled
	  ND DAD is enabled, number of DAD attempts: 1
	  ND reachable time is 30000 milliseconds
	  ND advertised reachable time is 0 milliseconds
	  ND retransmit interval is 1000 milliseconds

Configuration Steps	Change the IPv6 MTU of interface GigabitEthernet 0/0 to 1,300.
	FS(config-if-GigabitEthernet 0/0)#ipv6 mtu 1300
Verification	Run the **show ipv6 interface** command to check whether the configuration takes effect.
	ND advertised retransmit interval is 0 milliseconds ND router advertisements are sent every 200 seconds<160--240> ND router advertisements live for 1800 seconds

Configuring the Static PMTU

Configuration Steps	Set the PMTU of IPv6 address A000::1 to 1,400 bytes.
	FS(config)#ipv6 path-mtu A000::1 1400
Verification	Run the **show ipv6 path-mtu** command to check whether the configuration takes effect.
	FS#show ipv6 path-mtu IPv6 Address MTU Age Type A000::1 1400 -- Static A000::2 1300 1 Dynamic Age indicates the aging time, that is, the length from the time when dynamic PMTUs are learned to the current time. The unit is minute. If static PMTUs are learned, the value of Age is represented by (--). Types indicates the PMTU type: dynamic or static.

Configuring the Aging Time of the Dynamic PMTU

Configuration Steps	Set the aging time of the dynamic PMTU to 30 minutes.
	FS(config)#ipv6 path-mtu age 30
Verification	Run the **show run** command to check whether the configuration takes effect.
	FS#show run | include ipv6 path-mtu age ipv6 path-mtu age 30

1.4.5 Enabling IPv6 Source Routing

Configuration Effect

RFC 5095 abolished the Type 0 routing header. FS devices do not support the Type 0 routing header by default. The administrator can run the **ipv6 source-route** command to in global configuration mode to enable IPv6 source routing.

Configuration Steps

Enabling IPv6 Source Routing

Optional.

To enable IPv6 source routing, run the ipv6 source-route command.

Verification

The device can properly forward packets carrying the Type 0 routing header.

Related Commands

Enabling IPv6 Source Routing

Command	**ipv6 source-route**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Since the Type 0 header may cause the device prone to DoS attacks, the device does not forward IPv6 packets carrying the routing header by default, but still processes IPv6 packets with itself being the final destination address and the Type 0 routing header.

Configuration Example

Enabling IPv6 Source Routing

Configuration Steps	Enable IPv6 source routing.
	FS(config)#ipv6 source-route
Verification	Run the **show run** command to check whether the configuration takes effect.
	FS#show run | inc ipv6 source-route ipv6 source-route

1.4.6 Configuring the Sending Rate of ICMPv6 Error Messages

Configuration Effect

Configure the sending rate of ICMPv6 error messages.

Configuration Steps

Configuring the Sending Rate of ICMPv6 Packet Too Big Messages

Optional.

If a device receives many IPv6 packets with the packet length exceeding the IPv6 MTU of the outbound interface and thereby sends many ICMPv6 Packet Too Big messages to consume much CPU resources, run the ipv6 icmp error-interval too-big command to restrict the sending rate of this error message.

Configuring the Sending Rate of Other ICMPv6 Error Messages

Optional.

If a device receives many illegal IPv6 packets and thereby generates many ICMPv6 error messages, run the ipv6 icmp error-interval command to restrict the sending rate of ICMPv6 error messages. (This command does not affect the sending rate of ICMPv6 Packet Too Big messages.)

Verification

Run the **show running-config** command to check whether the configuration takes effect.

Related Commands

Configuring the Sending Rate of ICMPv6 Packet Too Big Messages

Command	**ipv6 icmp error-interval too-big** *milliseconds* [*bucket-size*]
Parameter Description	*milliseconds*: Indicates the refresh period of a token bucket, ranging from 0 to 2,147,483,647. The unit is millisecond. The default value is 100. If the value is 0, the sending rate of ICMPv6 error messages is not restricted. *bucket-size*: Indicates the number of tokens in a token bucket, ranging from 1 to 200. The default value is 10.
Command Mode	Global configuration mode
Usage Guide	To prevent DoS attacks, use the token bucket algorithm to restrict the sending rate of ICMPv6 error messages. If the length of an IPv6 packet to be forwarded exceeds the IPv6 MTU of the outbound interface, the router discards this IPv6 packet and sends back an ICMPv6 Packet Too Big message to the source IPv6 address. This error message is mainly used as part of the IPv6 PMTUD process. If other ICMPv6 error messages are excessive, ICMPv6 Packet Too Big messages cannot be sent, causing failure of IPv6 PMTUD. Therefore, it is recommended to restrict the sending rate of ICMPv6 Packet Too Big messages independently of other ICMPv6 error messages. Since the precision of the timer is 10 milliseconds, it is recommended to set the refresh period of a token bucket to an integer multiple of 10 milliseconds. If the refresh period of the token bucket is between 0 and 10, the actual refresh period is 10 milliseconds. For example, if the sending rate is set to 1 every 5 milliseconds, two error messages are sent every 10 milliseconds in actual situations. If the refresh period of the token bucket is not an integer multiple of 10 milliseconds, it is automatically converted to an integer multiple of 10 milliseconds. For example, if the sending rate is set to 3 every 15 milliseconds, two tokens are refreshed every 10 milliseconds in actual situations.

Configuring the Sending Rate of Other ICMPv6 Error Messages

Command	**ipv6 icmp error-interval** *milliseconds* [*bucket-size*]
Parameter Description	*milliseconds*: Indicates the refresh period of a token bucket, ranging from 0 to 2,147,483,647. The unit is millisecond. The default value is 100. If the value is 0, the sending rate of ICMPv6 error messages is not restricted. *bucket-size*: Indicates the number of tokens in a token bucket, ranging from 1 to 200. The default value is 10.
Command	Global configuration mode

Mode	
Usage Guide	To prevent DoS attacks, use the token bucket algorithm to restrict the sending rate of ICMPv6 error messages. Since the precision of the timer is 10 milliseconds, it is recommended to set the refresh period of a token bucket to an integer multiple of 10 milliseconds. If the refresh period of the token bucket is between 0 and 10, the actual refresh period is 10 milliseconds. For example, if the sending rate is set to 1 every 5 milliseconds, two error messages are sent every 10 milliseconds in actual situations. If the refresh period of the token bucket is not an integer multiple of 10 milliseconds, it is automatically converted to an integer multiple of 10 milliseconds. For example, if the sending rate is set to 3 every 15 milliseconds, two tokens are refreshed every 10 milliseconds in actual situations.

Configuration Example

Configuring the Sending Rate of ICMPv6 Error Messages

Configuration Steps	Set the sending rate of the ICMPv6 Packet Too Big message to 100 pps and that of other ICMPv6 error messages to 10 pps.
	FS(config)#ipv6 icmp error-interval too-big 1000 100 FS(config)#ipv6 icmp error-interval 1000 10
Verification	Run the **show running-config** command to check whether the configuration takes effect.
	FS#show running-config | include ipv6 icmp error-interval ipv6 icmp error-interval 1000 10 ipv6 icmp error-interval too-big 1000 100

1.4.7 Configuring the IPv6 Hop Limit

Configuration Effect

Configure the number of hops of a unicast packet to prevent the packet from being unlimitedly transmitted.

Configuration Steps

Configuring the IPv6 Hop Limit

Optional.
To modify the number of hops of a unicast packet, run the ipv6 hop-limit value command.

Verification

Run the show running-config command to check whether the configuration is correct.
Capture the IPv6 unicast packets sent by a host. The packet capture result shows that the hop-limit field value in the IPv6 header is the same as the configured hop limit.

Related Commands

Configuring the IPv6 Hop Limit

Command	**ipv6 hop-limit value**
Parameter Description	*value*: Indicates the number of hops of a unicast packet sent by the device. The value ranges from 1 to 255.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the IPv6 Hop Limit

Configuration Steps	Change the IPv6 hop limit of a device to 250.
	FS(config)#ipv6 hop-limit 250
Verification	Run the **show running-config** command to check whether the configuration takes effect.
	FS#show running-config ipv6 hop-limit 254

1.4.8 Enabling/Disabling the Function of Refraining from Sending NS Packets to Authentication VLANs

Configuration Effect

Enable or disable the function of refraining from sending NS packets to authentication VLANs on an SVI.

Notes

The configuration is supported only on SVIs and takes effect only in gateway authentication mode.

Configuration Steps

Enabling/Disabling the Function of Refraining from Sending NS Packets to Authentication VLANs

Optional.

In gateway authentication mode, run the no ipv6 nd suppress-auth-vlan-ns command so that the device can send NS packets to authentication VLANs.

Verification

Run the show running-config command to check whether the configuration is correct.

Related Commands

Enabling/Disabling the Function of Refraining from Sending NS Packets to Authentication VLANs

Command	**ipv6 nd suppress-auth-vlan-ns**
Parameter	N/A

Description	
Command Mode	Interface configuration mode
Usage Guide	Use the **no** form of this command to disable this function.

Configuration Example

Disabling the Function of Refraining from Sending NS Packets to Authentication VLANs

Configuration Steps	Disable the function of refraining from sending NS packets to authentication VLANs.
	FS(config-if-VLAN 2)#no ipv6 nd suppress-auth-vlan-ns
Verification	Run the **show running-config interface vlan 2** command to check whether the configuration takes effect.
	FS#show running-config interface vlan 2 no ipv6 nd suppress-auth-vlan-ns

1.4.9 Configuring the Default Gateway on the Management Interface

Configuration Effect

Configure the default gateway on the management interface. A default route is generated, with the outbound interface being the management interface and the next hop being the configured gateway.

Notes

The configuration is supported only on the management interface.

Configuration Steps

Configuring the Default Gateway on the Management Interface

Optional.
To configure a default route and the next hop for the management interface, run the ipv6 gateway command.

Verification

Run the show running-config command to check whether the configuration is correct.

Related Commands

Configuring the Default Gateway on the Management Interface

Command	**ipv6 gateway** *ipv6-address*
Parameter Description	N/A
Command	Interface configuration mode

Mode	
Usage Guide	This command is supported only on the management interface.

Configuration Example

Configuring the Default Gateway on the Management Interface

Configuration Steps	Sett the default gateway of the management interface to 2000::1.
	FS(config)# interface mgmt 0 FS(config-mgmt)# ipv6 gateway 2000::1
Verification	Run the **show running-config interface vlan 2** command to check whether the configuration takes effect.
	FS#show running-config interface mgmt 0 Ipv6 gateway 2000::1

1.4.10 Configuring the IPv6 ND to Allocate Different Prefixes to Different Users

Configuration Effect

Configure a specific prefix pool for an interface to ensure that different IPv6 prefixes are allocated to different users under this interface.

Configuration Steps

Binding Prefix to Interface

Optional.
In global configuration mode, run the ipv6 local pool pool-name ipv6-prefix/prefix-length prefix-length command to configure an allocable prefix pool.
In interface configuration mode, run the ipv6 nd prefix pool pool-name command to bind a prefix pool name to the interface.

Verification

Run the show running-config command to check whether the configuration is correct.

Related Commands

Binding Prefix to Interface

Command	**ipv6 local pool** *pool-name ipv6-prefix/prefix-length prefix-length*
Parameter Description	-
Command Mode	Interface configuration mode
Usage Guide	pool-name specifies the prefix pool configured by running the **ipv6 local pool** *pool-name* ***ipv6-prefix/prefix-length***

	prefix-length command.

Configuration Example

Binding Prefix to Interface

Configuration Steps	Bind the prefix FS to the VLAN 1 interface to ensure that users under VLAN 1 are allocated different address prefixes based on the prefix FS.
	FS(config)# ipv6 local pool FS 2409:88A0:8205::/48 64 FS(config)# interface vlan 1 FS(config-if-VLAN 1)# ipv6 nd prefix pool FS
Verification	Run the **show running-config interface vlan 1** command to check whether the configuration takes effect.
	FS#show running-config interface vlan 1 ipv6 nd prefix pool FS

1.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears the dynamically learned neighbors.	**clrear ipv6 neighbors** [**vrf***vrf-name*] [**oob**] [*interface-id*] **clrear ipv6 neighbors** [**vrf***vrf-name*] [*interface-id*] **clrear ipv6 neighbors** [*interface-id*]
Clears the dynamic PMTU.	**clear ipv6 path-mtu** [**vrf** *vrf-name*] [*ipv6-address*] **clear ipv6 path-mtu**[*ipv6-address*] **clear ipv6 path-mtu all**/Clears the dynamic PMTU of the public network and all VRF instances.

Displaying

Description	Command
Displays IPv6 information of an interface.	**show ipv6 interface** [[*interface-id*] [ra-info]] [brief [*interface-id*]]
Displays neighbor information.	**show ipv6 neighbors[vrf***vrf-name*] [**verbose**][*interface-id*] [*ipv6-address*] [static] [oob] **show ipv6 neighbors[vrf***vrf-name*] [**verbose**][*interface-id*] [*ipv6-address*] [static] **show ipv6 neighbors** [**verbose**][*interface-id*] [*ipv6-address*] [static]
Displays the number of ND entries corresponding to each MAC address.	**show ipv6 neighbor statistics per-mac** [*interface-name*] [*mac-address*]
Displays the PMTU.	**show ipv6 path-mtu** [**vrf***vrf-name*][*ipv6-address* /**dynamic** /**static**] **show ipv6 path-mtu** [*ipv6-address* /**dynamic** /**static**]
Displays the PMTU statistics.	**show ipv6 path-mtu statistics**

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs ND entry learning.	**debug ipv6 nd**

Chapter 8 Network Management Configuration

1. Configuring RLOG
2. Configuring Police Log
3. Configuring Log Policy
4. Configuring SNMP
5. Configuring CM-APM
6. ANTI-SNIPER

1 Configuring RLOG

1.1 Overview

Remote Log (RLOG) is developed for the device to upload its collected logs to the remote server (for example, the ELOG or SNC server).

The server parses the logs and writes them into the database.

RLOG can upload multiple types of logs, such as device running logs, Internet access logs, and system security logs. The logs can be queried on the server.

Protocols and Standards

- N/A

1.2 Applications

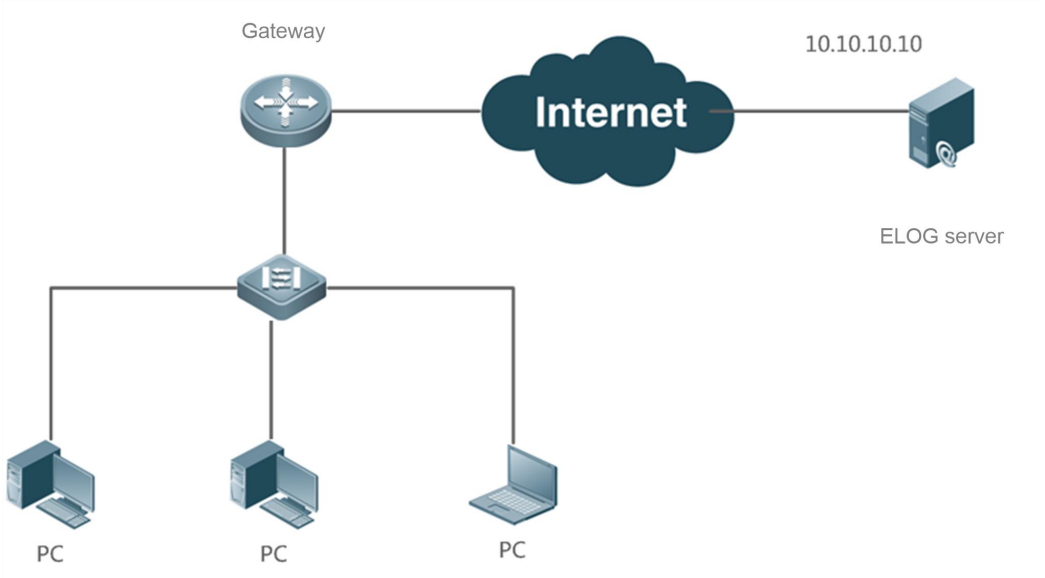
Application	Description
NAT Log Export	After NAT logging is enabled, RLOG can export NAT logs to the server, so that details of each data flow can be queried on the server.

1.2.1 NAT Log Export

Scenario

With RLOG and NAT logging enabled on the gateway, NAT logs are generated when a user accesses the Internet from the gateway. When a flow is closed, NAT logs are exported to the ELOG server via RLOG.

Figure 1-1



Deployment

- On the gateway, enable NAT logging and RLOG, and configure the RLOG server.

- Enable the RLOG server to receive and parse logs for statistics queries.

1.3 Features

Basic Concepts

N/A

Overview

Feature	Description
RLOG Export	Exports logs from the gateway to the server.
RLOG-specific Server	Configures a separate RLOG server for each type of logs.

1.3.1 RLOG Export

Device logs are exported to the RLOG server.

Working Principle

The flow log module, device audit module, traffic audit module, content audit module, and other function modules of the device generate corresponding logs, and the logs are sent to the server via the RLOG interface. The server receives, parses, and displays these logs.

Related Configuration

Enabling a Log Module

A log module is disabled by default, and needs to be enabled first when required.

For example, the traffic audit log module needs to be enabled by running the **flow-audit enable** command.

Configuring RLOG

No RLOG server or export function is configured by default.

To configure a server, run the **rlog server 192.168.1.100 port 20000** command.

To export logs to the server, run the **rlog type 25 server 192.168.1.100 priority 1** command.

The parameter **type 25** indicates interface traffic logs.

1.3.2 RLOG-specific Server

Different types of logs are exported to different servers.

Working Principle

When receiving log sending requests from log modules, RLOG handles different types of logs according to configurations.

Related Configuration

Enabling a Log Module

A log module is disabled by default, and needs to be enabled first when required.

For example, the traffic audit log module needs to be enabled by running the **flow-audit enable** command.

Configuring RLOG

No RLOG server or export function is configured by default.

To configure two servers, run the following commands:

rlog server 192.168.1.100 port 20000

rlog server 192.168.1.101 port20000

To send flow logs to the server, run the **rlog type 16 server 192.168.1.100 priority 1** command. The parameter **type 16** indicates flow logs.

To send interface traffic logs to the server, run the **rlog type 25 server 192.168.1.101 priority 1** command.

1.4 Configuration

Configuration	Description and Command	
Configuring RLOG Export	(Mandatory) It is used to specify the RLOG server address and port.	
	rlog server *ip-address* [**oob**] [**port***port-num*]	Specifies the RLOG server IP address and management port for exporting logs, and enables RLOG export. The default port is Port 20000.
	rlog type *n***server** *server-ip* **priority** *prio*	Specifies the RLOG type and the priority for a specific server.
Configuring RLOG Parameters	(Optional) It is used to specify the RLOG export rate.	
	rlog export-rate *val*	Specifies the RLOG export rate (maximum number of logs sent per second).
	rlog set log-com	Specifies whether to enable RLOG combination for export.
	rlog dev-ip*ip*	Specifies the IP address of the RLOG device.
	rlog sn-mac-on	Configures flow logs to carry the SN and MAC address.
	rlog filter*acl_id*	Configures RLOG filtering conditions. This command is currently not supported.
Configuring RLOG File Export	(Optional) It is used to configure log export to the RLOG server in file mode.	
	rlog-file server *protocolip-address* [**port***port-num*] [**oob**] [**path***server-path-string*] [**username***username-string***passwd***passwd-string*]	Configures the RLOG file server.
	rlog-file local-path *path-string*	Configures the local cache path for RLOG files.
	rlog-file storage *storage-size*	Configures the size of the local cache for storing RLOG files.

	rlog-file send time-range from *from-hour* **to** *to-hour* **rlog-file send compress { zip | none }** **rlog-file send format {elog | macc }**	Sets the RLOG file export parameters.
	rlog-file type *type-num*	Sets the RLOG file type.
Configuring NAT Logging	(Optional) It is used to record NAT logs.	
	nat-log enable	Enables NAT logging.
	ip nat-log on	Enables NAT logging to record only NAT logs.

1.4.1 Configuring RLOG Export

Configuration Effect

- Configure the RLOG server.
- Configure the RLOG type.

Notes

- N/A

Configuration Steps

Configuring the RLOG Server

- Mandatory.
- Configure one server unless otherwise specified.

Configuring the RLOG Type

- Mandatory.
- Configure the RLOG type as required.

Verification

Check whether the device sends logs properly.

- Check whether the RLOG server successfully receives each log packet.

Related Commands

Configuring the RLOG Server

Command	**rlog server** *ip-address*[**oob**] [**port***port-num*]
Parameter Description	*Ip-address*: Indicates the IP address of the RLOG server. *port-num*: Indicates the port ID of the RLOG server. **Oob**: Indicates the OOB interface.
Command Mode	Global configuration mode

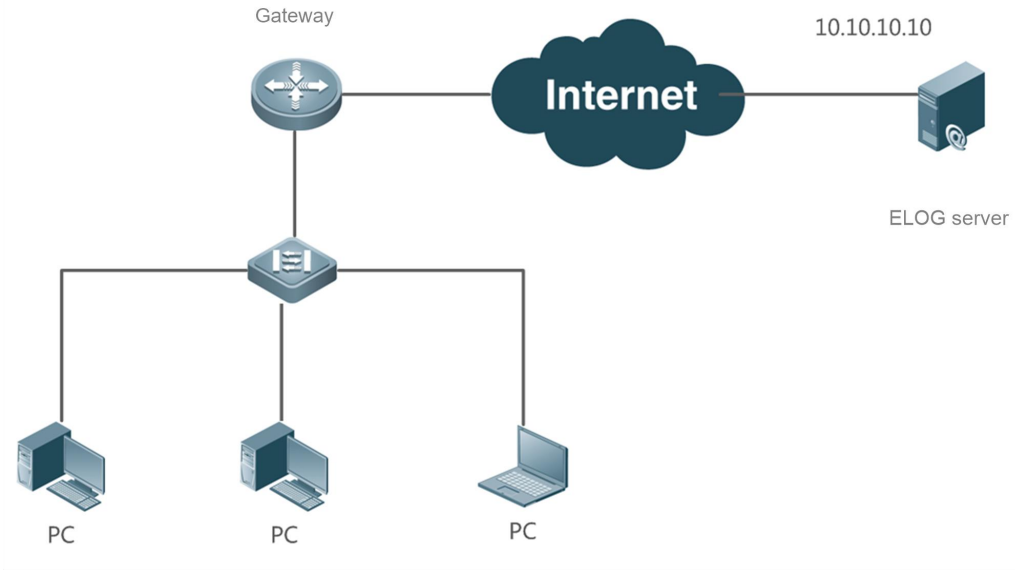
Usage Guide	This command only enables the RLOG service. No log is output if only this command is executed. For example, to separately enable flow logging, run the **ip session log-on** command. To cancel the server configuration, run the **no rlog server***ip-address* command.

Configuring the RLOG Type

Command	**rlog type** *n***server** *server-ip* **priority** *prio* **rlog type** *n* **file**
Parameter Description	*n*: Indicates the RLOG type. *server-ip*: Indicates the IP address of the RLOG server. *prio*: Indicates the RLOG priority. The value ranges from 0 to 7. A smaller value indicates a higher priority. **rlog type** *n* **file**: Indicates that log files are directly generated, which are sent via the RLOG-FILE module.
Command Mode	Global configuration mode
Usage Guide	To cancel export of a specific RLOG type, run the **no rlog type***n***server***srever-ip* command. Currently supported RLOG types are as follows: [16] RLOG_TYPE_FLOW, /* Flow logs */ [17] RLOG_TYPE_CPU_MEM, /* CPU and memory usage logs */ [18] RLOG_TYPE_DISC, /* Hard disk usage logs */ [19] RLOG_TYPE_DEV_LOG, /* Device audit logs */ [20] RLOG_TYPE_URL_AUDIT, /* URL audit logs */ [21] RLOG_TYPE_SESSION, /* Online IP address and session count logs */ [22] RLOG_TYPE_IP_APP, /* IP-specific application traffic logs */ [23] RLOG_TYPE_IP, /* IP-specific session count logs */ [24] RLOG_TYPE_CHANNEL, /* Channel-specific traffic logs */ [25] RLOG_TYPE_INTERFACE, /* Interface-specific traffic logs */ [26] RLOG_TYPE_IP_OFFLINE, /* IP address go-offline notification logs */ [27] RLOG_TYPE_MAIL_AUDIT, /* E-mail audit logs */ [28] RLOG_TYPE_TELNET_AUDIT, /* Telnet audit logs */ [29] RLOG_TYPE_WEB_SEARCH_AUDIT, /* Web search audit logs */ [30] RLOG_TYPE_WEB_BBS_AUDIT, /* Web BBS audit logs */ [31] RLOG_TYPE_IM_AUDIT, /* IM audit logs */ [32] RLOG_TYPE_FTP_AUDIT, /* FTP audit logs */ [33] RLOG_TYPE_WEB_AUDIT, /* Web audit logs */ [34] RLOG_TYPE_APP_AUDIT, /* Application control audit logs */ [35] RLOG_TYPE_FLOOD, /* Flood attack detection logs */ [36] RLOG_TYPE_FLOOD_CEASEm, /* Flood attack cease logs*/ [37] RLOG_TYPE_SCAN, /* Scan detection logs */ [38] RLOG_TYPE_SCAN_CEASE, /* Scan cease logs*/ [39] RLOG_TYPE_ATTACK_FRAG, /* IP fragmentation attack detection logs */

Configuration Example

Configuring Flow Log Export to the Server at 10.10.10.10

Scenario **Figure 1-1**	
Configuration Steps	● Configure the IP address and port of the RLOG server on the gateway. ● On the gateway, configure flow log export to the RLOG server at 10.10.10.10. ● Enable flow logging on the gateway.
A	A#configure terminal A(config)#rlog server 10.10.10.10 port 20000 A(config)# rlog type 16 server 10.10.10.10 priority 1 A(config)#ip session log-on
Verification	Check whether the gateway sends log packets to the RLOG server, or check whether the exported log count of RLOG increases. ● Check whether the generated log count of RLOG increases. ● Check whether the export log count of RLOG increases
A	A# show rlog-status log local rlog message: remote rlog message: [16]RLOG_TYPE_FLOW : 0 [17]RLOG_TYPE_CPU_MEM : 0 [18]RLOG_TYPE_DISC : 0 [19]RLOG_TYPE_DEV_LOG : 0 [20]RLOG_TYPE_URL_AUDIT : 0

	[21]RLOG_TYPE_SESSION : 0 [22]RLOG_TYPE_IP_APP : 0 [23]RLOG_TYPE_IP : 0 [24]RLOG_TYPE_CHANNEL : 0 [25]RLOG_TYPE_INTERFACE : 0 [26]RLOG_TYPE_IP_OFFLINE : 0 [27]RLOG_TYPE_MAIL_AUDIT : 0 [28]RLOG_TYPE_TELNET_AUDIT : 0 [29]RLOG_TYPE_WEB_SEARCH_AUDIT : 0 [30]RLOG_TYPE_WEB_BBS_AUDIT : 0 [31]RLOG_TYPE_IM_AUDIT : 0 [32]RLOG_TYPE_FTP_AUDIT : 0 [33]RLOG_TYPE_WEB_AUDIT : 0 [34]RLOG_TYPE_APP_AUDIT : 0 [35]RLOG_TYPE_FLOOD : 0 [36]RLOG_TYPE_FLOOD_CEASEm : 0 [37]RLOG_TYPE_SCAN : 0 [38]RLOG_TYPE_SCAN_CEASE : 0 [39]RLOG_TYPE_ATTACK_FRAG : 0 If a log is generated, the **RLOG_TYPE_FLOW** value increases.
A	A# show rlog rlog server is enable port 20000 server 192.168.1.100 port 20000 server 10.10.10.10 rlog dev-ip 0.0.0.0 rlog export-rate 10000 rlog queue remain 10000 send log count : 0 error count : 0 errorno : 0 recv buf: 0 poll buf err: 0 push buf: 0 local buf: 0 recv err cnt: 0 depatch err cnt: 0 enable log combination: 0 If a log is successfully exported, the **send log count** value increases.

Common Errors

- The RLOG server is configured, but the RLOG type is not specified.
- The RLOG server and type are configured, but the log module is not enabled.

1.4.2 Configuring RLOG Parameters

Configuration Effect

- Enable RLOG to operate with better performance.

Notes

- Fully understand each command parameter before the configuration; otherwise, RLOG may malfunction.

Configuration Steps

- Configure RLOG parameters as required.

Verification

- Check whether RLOG properly exports logs and the server properly receives the logs.

Related Commands

Configuring the RLOG Export Rate

Command	**rlog export-rate** *val*
Parameter Description	*val*: Indicates the RLOG export rate (the maximum number of logs sent per second).
Command Mode	Global configuration mode
Usage Guide	The RLOG export rate is determined by device and server performance as well as log outputs. An excessively low rate causes log losses, while an excessively high rate continuously raises CPU usage.

Configuration RLOG Combination

Command	**rlog set log-com**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	With this function enabled, multiple logs are combined in one packet. Check whether the RLOG server supports this function before configuration.

Configuring the IP Address of the RLOG Device

Command	**rlog dev-ip** *ip*
Parameter Description	*ip*: Indicates the IP address of the RLOG device.

Command Mode	Global configuration mode
Usage Guide	The IP address of the RLOG device is required for exporting specific types of logs. Configure this function as required.

Configuring RLOG Filtering Conditions

Command	**rlog filter***acl_id*
Parameter Description	access-list id
Command Mode	Global configuration mode
Usage Guide	This command is currently not supported.

Configures Flow Logs to Carry the SN and MAC Address

Command	**rlog sn-mac-on**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Enable this function only after confirming that the server supports the log format.

Configuration Example

Specifying the IP Address of the RLOG Device to 10.10.10.1, and RLOG Export Rate to 10000, Without RLOG Combination

Configuration Steps	
	FS#configure terminal FS(config)# rlog dev-ip 10.10.10.1 FS(config)# rlog export-rate 10000 FS(config)# end
Verification	Check whether the configuration takes effect and whether the RLOG server receives logs properly.

	FS# show rlog
	rlog server is enable
	  port 20000 server 192.168.1.100
	  port 20000 server 10.10.10.10
	rlog dev-ip 10.10.10.1
	rlog export-rate 10000 rlog queue remain 10000
	send log count : 0 error count : 0 errorno : 0

	recv buf: 0 poll buf err: 0 push buf: 0 local buf: 0 recv err cnt: 0 depatch err cnt: 0

Common Errors

- The RLOG export rate is excessively small, and logs are lost.

1.4.3 Configuring RLOG File Export

Configuration Effect

- Configure the RLOG file server.
- Configure the RLOG file type.

Notes

- N/A

Configuration Steps

Configure the RLOG File Server

- Mandatory.
- Only one RLOG file server can be configured.

Configuring the RLOG File Type

- Mandatory.
- Configure the RLOG type as required.

Verification

Check whether the device sends logs properly.

- Check whether the RLOG server successfully receives each log file.

Related Commands

Configuring the RLOG File Server

Command	**rlog-file server** *protocol ip-address* [**port** *port-num*] [**oob**] [**path** *server-path-string*] [**username** *username-string* **passwd** *passwd-string*]
Parameter Description	*protocol*: Indicates HTTP or FTP. *ip-address*: Indicates the IP address of the RLOG file server. *port-num*: Indicates the service port of the RLOG file server. This port is applicable only in HTTP mode. The default port is Port 80. **oob**: Indicates the OOB interface, which is available only in HTTP mode. *server-path-string*: Indicates the server path. The default path is **l**. *username-string*: indicates the username. The default value is **FS**.

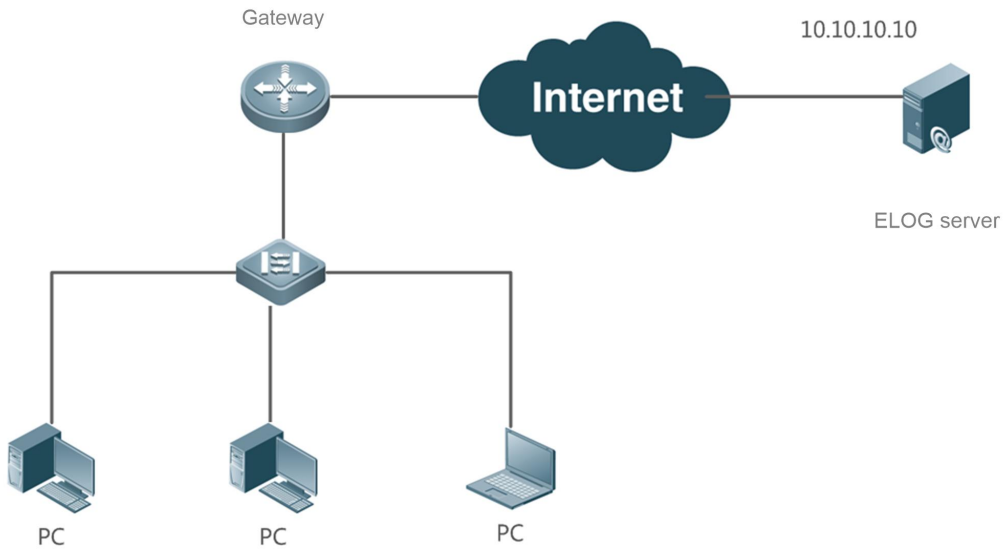
	passwd-string: indicates the password. The default value is **FS**.
Command Mode	Global configuration mode
Usage Guide	This command only enables the log file service. No log is output if only this command is executed. To cancel the server configuration, run the **no rlog-file server***ip-address* command.

Configuring the RLOG File Type

Command	**rlog-file type** *type-num*
Parameter Description	type-num: Indicates the RLOG file type.
Command Mode	Global configuration mode
Usage Guide	To cancel export of a specific RLOG file type, run the **no rlog-file type***n* command. Currently supported RLOG file types are as follows: [16] RLOG_TYPE_FLOW, /* Flow logs */ [17] RLOG_TYPE_CPU_MEM, /* CPU and memory usage logs */ [18] RLOG_TYPE_DISC, /* Hard disk usage logs */ [19] RLOG_TYPE_DEV_LOG, /* Device audit logs */ [20] RLOG_TYPE_URL_AUDIT, /* URL audit logs */ [21] RLOG_TYPE_SESSION, /* Online IP address and session count logs */ [22] RLOG_TYPE_IP_APP, /* IP-specific application traffic logs */ [23] RLOG_TYPE_IP, /* IP-specific session count logs */ [24] RLOG_TYPE_CHANNEL, /* Channel-specific traffic logs */ [25] RLOG_TYPE_INTERFACE, /* Interface-specific traffic logs */ [26] RLOG_TYPE_IP_OFFLINE, /* IP address go-offline notification logs */ [27] RLOG_TYPE_MAIL_AUDIT, /* E-mail audit logs */ [28] RLOG_TYPE_TELNET_AUDIT, /* Telnet audit logs */ [29] RLOG_TYPE_WEB_SEARCH_AUDIT, /* Web search audit logs */ [30] RLOG_TYPE_WEB_BBS_AUDIT, /* Web BBS audit logs */ [31] RLOG_TYPE_IM_AUDIT, /* IM audit logs */ [32] RLOG_TYPE_FTP_AUDIT, /* FTP audit logs */ [33] RLOG_TYPE_WEB_AUDIT, /* Web audit logs */ [34] RLOG_TYPE_APP_AUDIT, /* Application control audit logs */ [35] RLOG_TYPE_FLOOD, /* Flood attack detection logs */ [36] RLOG_TYPE_FLOOD_CEASEm, /* Flood attack cease logs*/ [37] RLOG_TYPE_SCAN, /* Scan detection logs */ [38] RLOG_TYPE_SCAN_CEASE, /* Scan cease logs*/ [39] RLOG_TYPE_ATTACK_FRAG, /* IP fragmentation attack detection logs */

Configuration Example

Configuring Flow Log Export to the Server at 10.10.10.10

Scenario **Figure 1-3**	
Configuration Steps	● Configure the IP address and port of the RLOG file server on the gateway. ● On the gateway, configure e-mail audit logs and NAT logs to be exported to the server at 10.10.10.10 in FTP mode. ● Enable e-mail audit logging on the gateway.
A	A#configure terminal A(config)#rlog-file server 10.10.10.10 username test passwd test A(config)# rlog-file send protocol http A(config)# rlog-file type 48 A(config)#rlog type 16 file
Verification	Check whether the gateway sends log files to the RLOG file server, or check whether the exported log file count of RLOG increases.
A	A# show rlog-file info FS#showrlog-fileinfo rlog file server: http ip :172.18.8.97, port:8080 source :0.0.0.0 path : /ELCService/upload/PullLogFile username:; passwd:; local path : /mnt/usb0/rlog_file local storage : 524288 K send time-rage: from 0 to 24

	send compress : zip send format : ELOG client count : 3 LOG : total[2771]; tar[2771|0]; send[2771|0],lasterr[0] MAIL_BODY : total[2]; tar[2|0]; send[2|0],lasterr[0] MAIL_ATTACH: total[1]; tar[1|0]; send[1|0],lasterr[0] WEBMAIL : total[0]; tar[0|0]; send[0|0],lasterr[0] BSS_BODY : total[7]; tar[7|0]; send[7|0],lasterr[0] MACC : total[0]; tar[0|0]; send[0|0],lasterr[0] type RLOG_FILE_TYPE_MAIL_AUDIT 48 RLOG_FILE_TYPE_WEBMAIL_AUDIT 49 RLOG_FILE_TYPE_WEB_BBS_AUDIT 50 RLOG_FILE_TYPE_IP_APP 51 If a log file is generated, the **RLOG_FILE_TYPE_MAIL_AUDIT** value increases.

Common Errors

- The RLOG file server is configured, but the RLOG file type is not specified.
- The RLOG file server is configured, but information such as the username, password, transmission mode, compression mode, and file format is not configured.

1.4.4 Configuring NAT Logging

Configuration Effect

- Enable or disable NAT logging.

Notes

- Configure NAT logging as required.

Configuration Steps

- Configure NAT logging directly on a device requiring this function.

Verification

- Run the **show nat-log** command to check whether NAT logs exist.

Related Commands

Enabling NAT Logging

Command	**nat-log enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Enable this function to save NAT logs to local disks. Run the **no nat-log enable** command to cancel this configuration.

Setting the NAT Log Storage Period in Days

Command	**nat-log data-store** *days*
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure this command to set the NAT log storage period in days. The value ranges from 10 to 90.

Recording NAT Logs Only

Command	**ip nat-log on**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure this command to record only NAT logs in local disks. Run the **no ip nat-log on** command to disable this function. After this function is disabled, all flow logs are recorded.

Configuration Example

Enabling NAT Logging, Recording Only NAT Logs, and Setting the NAT Log Storage Period to 14 Days

Configuration Steps	
	FS#configure terminal FS(config)# ip nat-log on FS(config)#nat-log enable FS(config)# nat-log data-store 14 FS(config)# end
Verification	Assuming that flows are properly generated and closed and the date is 2014-4-16, check whether NAT logs are displayed.

Common Errors

- NAT logging is disabled.

1.5 Monitoring

Clearing

N/A

Displaying

Description	Command
Displays RLOG running and configuration information.	**show rlog**
Displays supported RLOG types.	**show rlog-type**
Displays the status of the RLOG server.	**show rlog-status** [**server** *ip*]
Displays the number of clients connected to RLOG.	**show rlog-status client**
Displays the log count of each RLOG type.	**show rlog-status log**
Displays flow/NAT logs in a specific period by username, protocol, source IP address, source port, destination IP address, and destination port.	**Show nat-log**[**username** *user_name*] [**ip-protocol** *ip-protocol*] [**source-ip** *source-ip*] [**dst-ip** *dst-ip*] [**src-port** *src-port*] [**dst-port** *dst-port*] **time-interval** *begin-year begin-mon begin-day begin-hour* **to** *end-year end-mon end-day end-hour*

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs RLOG.	**debug rlog info**
Debugs the RLOG library.	**debug rlog lib**
Debugs NAT logging.	**debug nat-log**

2 Configuring POLICE-LOG

2.1 Overview

POLICE-LOG is a program for managing public wireless network access security. It enables the gateway to interact with the MACC/ELOG or the third party and send logs as required.

In the public network access scenario with MACC/ELOG enabled, POLICE-LOG must be enabled to interconnect with the MACC/ELOG, so that the MACC/ELOG can interconnect with the network monitoring platform of the Ministry of Public Security.

Protocol Specifications

Network monitoring audit must be performed to guarantee public wireless network access security. To ensure better interconnection between products of manufacturers and the network monitoring system of the Ministry of Public Security, the Office of Cyber Security of the Ministry of Public Security puts forward the following standards:

GAWA3011.1-2015 Public Wireless Network Access Security Management System Functional Requirements for End of Wireless Access Places

GAWA3011.2-2015 Public Wireless Network Access Security Management System Functional Requirements for Management Background (Secret)

GAWA3011.3-2015 Public Wireless Network Access Security Management System Exchange Formats of Front-end Data and Basic Data

GAWA3011.4-2015 Public Wireless Network Access Security Management System Data Transmission and Exchange Specifications

GAWA3011.5-2015 Public Wireless Network Access Security Management System Unified XML Schema Port Specifications

2.2 Application

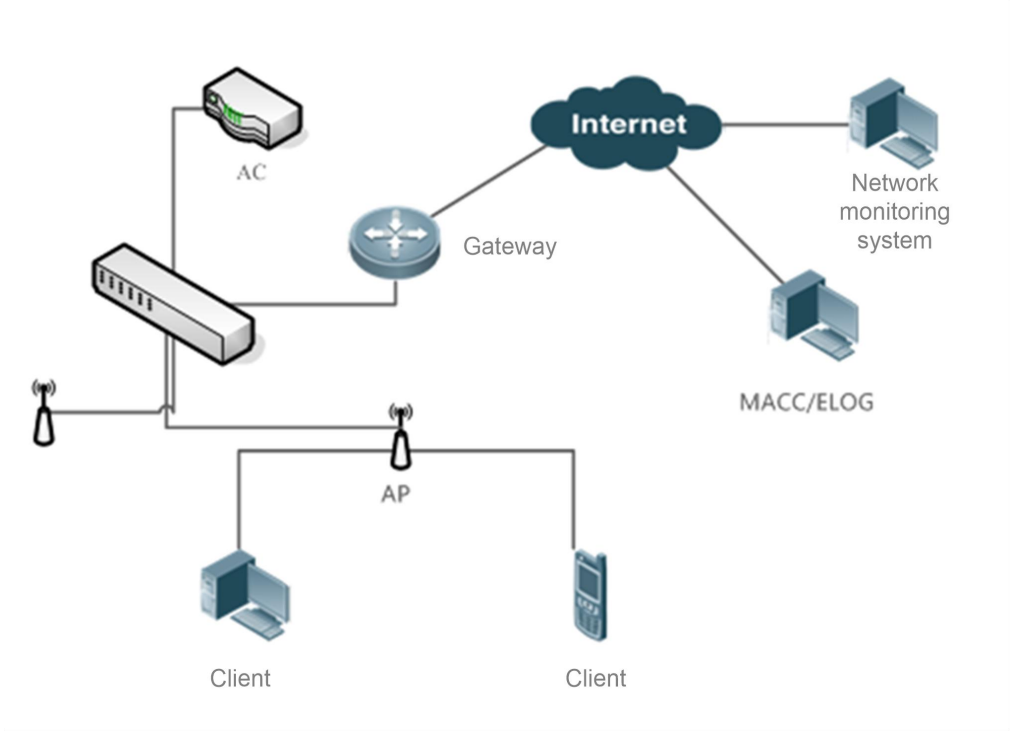
Application	Description
Applying Network Monitoring Audit	This function is applied to a common scenario complying with the public network access security standard.

2.2.1 Applying Network Monitoring Audit

Scenario

- The gateway serves as a NAT gateway.
- The MACC/ELOG can manage the gateway in terms of aspects such as remote update, status monitoring, and configuration delivery.
- The network monitoring system can receive audit logs of the MACC/ELOG.

Figure 1- 1



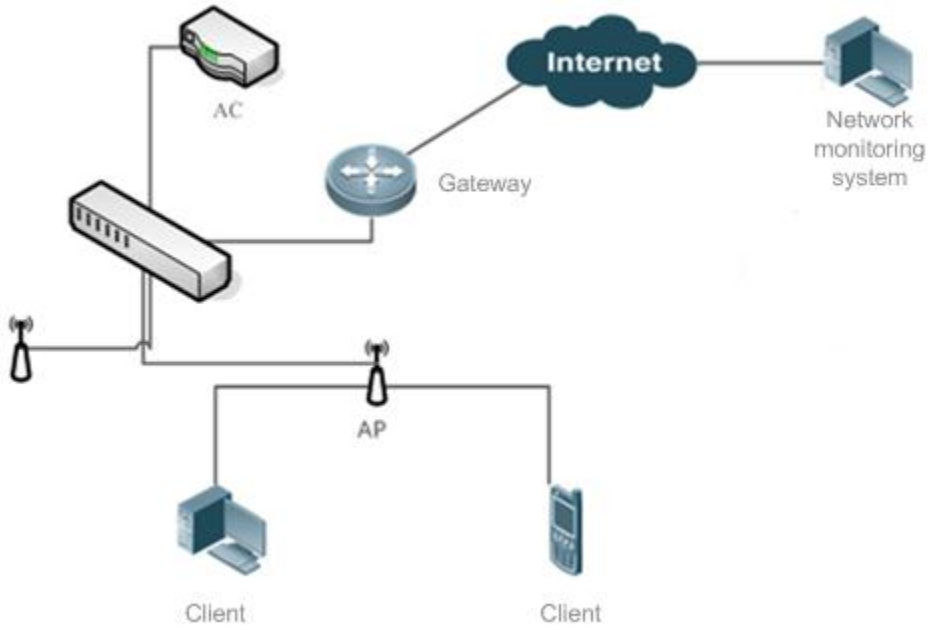
Deployment

- Enable POLICE-LOG on the gateway.
- Enable NAT-LOG on the gateway.
- Enable the general log component on the gateway.

Surfilter System Interconnection Scenario

- The gateway serves as a NAT gateway or a bypass.
- The Surfilter system can receive audit logs from the gateway.

Figure 1- 2



Deployment

- Enable POLICE-LOG on the gateway.
- Enable NAT-LOG on the gateway.
- Enable the general log component on the gateway.

2.3 Features

Basic Concepts

Authentication Log

A client needs to pass the real-name authentication before accessing the wireless network. The real name may be the user's ID card number or mobile phone number. Authentication logs will be sent to the network monitoring platform to track online behaviors of real-name users.

NAT Flow Log

The gateway provides the NAT function. To audit online behaviors of a specific client, the 5-tuple information (source address, source port, destination address, destination port, and protocol type) of NAT flows and the network access behavior details of the client must be audited.

General Log

As an egress device, the gateway provides the content audit function. It can audit online behaviors of a specific user, and output logs concerning the virtual identity, HTTP access, mail, Web BBS, and Web search for details about the user's online behaviors. These logs are called general logs.

Feature

Feature	Description
MACC Interconnection	The MACC needs to identify the interconnected device and detect its status.
Authentication Logs	A client accesses networks after authentication. The authentication logs must be reported to the MACC so that the network monitoring platform can track the client.
NAT Flow Logs	NAT flow logs are network access logs of clients, and are used by the network monitoring platform to analyze online behaviors of the clients.
General Logs	General logs are used to identify a user's online behaviors and are provided for the network monitoring platform for analysis and recording.

2.3.1 MACC Interconnection

The MACC needs to identify the interconnected device and detect its status.

Working Principle

When LOG_SERVER on the gateway is enabled, the gateway obtains site information of the current device from the MACC according to the MACC address for interconnection configured in the command line. If the site information is successfully obtained, LOG_SERVER periodically reports the gateway status. To register the device with the MACC, the device sends a registration request to the MACC, and the MACC stores the registration information of the device and approves the registration request on the device management page of the MACC.

After a client passes authentication of the gateway, the gateway must report the authentication log to the MACC.

2.3.2 Authentication Logs

Working Principle

APP-AUTH is responsible for client authentication. When a client goes offline, APP-AUTH sends the go-offline event to LOG_SERVER, so that LOG_SERVER changes the format of the go-offline event to the specified format and reports the go-offline event to the MACC. The MACC writes the go-offline event to the database, and displays it on the specified Web page.

2.3.3 NAT Flow Logs

NAT flow logs for network access of clients must be reported to the MACC. In this way, when the MACC interconnects with the network monitoring platform of the Ministry of Public Security, the network monitoring platform can extract concerned network behaviors based on the NAT flow logs.

Working Principle

NAT-LOG is registered with the flow platform. Upon flow creation, it obtains flow information and sends it to LOG_SERVER, which then changes the format of the flow information to the specified format and reports the flow information to the MACC. The MACC writes the flow information into the database and displays it on the specified Web page.

2.3.4 General Logs

General logs need to be reported to the MACC, which interconnects to the network monitoring platform of the Ministry of Public Security. In this way, the network monitoring platform can analyze the logs to identify network behaviors of users.

Working Principle

The content audit module identifies online behaviors of users from general logs concerning the virtual identity audit, mail audit, HTTP access audit, Web BBS audit, and Web search audit, and then sends the result to the network monitoring module police_log. The police_log module converts the format of the identification result and reports it to the MACC. The MACC stores the result into the database for display.

The virtual identity audit includes instant messaging (IM) chat audit and VID audit. The mail audit includes client mail audit and Web mail audit. The audit functions need to be enabled separately.

2.3.5 Direct Interconnection with Surfilter System

The FS device directly sends logs to the Surfilter system according to the Surfilter system interconnection specifications.

Working Principle

The FS device collects Internet access behavior identification logs in general logs, such as logs of the virtual identity audit, mail audit, HTTP access audit, Web BBS audit, and Web search audit. Subsequently, the FS device converts the logs into logs in the Surfilter log format according to the Surfilter system specifications, and then sends the logs to the Surfilter system for processing.

2.4 Configuration

Configuration	Description and Command	
Configuring Basic POLICE-LOG Function	Mandatory.	
	police-log enable	Enables POLICE-LOG module.
	police-log set url *url*	Configures MACC/ELOG address.
	police-log set second-url *url*	Configures the second MACC/ELOG address.
Enabling NAT-LOG Function	Mandatory.	
	nat-log police	Configures network monitoring NAT flow audit.
Configuring General Log Function	**content-audit write-plog** *im*	Enables the IM chat audit.
	#if !defined(CONFIG_EG_CA_NO_VID) && (!defined(CONFIG_EG_CA_SMALL_MEMORY) || defined(CONFIG_EG_CA_URL_DB_FLASH))	
	content-audit write-plog *vid*	Enables the VID audit.
	#endif	
	content-audit write-plog *mail*	Enables the client mail audit.
	content-audit write-plog *webmail*	Enables the Web mail audit.
	content-audit write-plog *url*	Enables the HTTP access audit.
	content-audit write-plog *webbbs*	Enables the Web BBS audit.
	content-audit write-plog websearch	Enables the Web search audit.
Configuring an Interconnection Platform	**police-log set platform**	Configures an interconnection platform.
Configuring Site Data	**netsite**	Configures site data.
	service-code	Configures the site code.

	service-type	Configures the site type.
	address	Configures the site address.
	longitude	Configures the site longitude.
	latitude	Configures the site latitude.
	business-nature	Configures the business nature of the site.
	status	Configures the business status.
	principal	Configures the business legal person of the site.
	principal-cert-type	Configures the valid certificate type of the business legal person.
	principal-cert-code	Configures the valid certificate number of the business legal person.
	principal-phone	Configures the contact information.
	start-time	Configures the business start time.
	end-time	Configures the business end time.
	producer-type	Configures the access type.
	producer-code	Configures the access service provider.
	province-code	Configures the province.
	city-code	Configures the city.
	area-code	Configures the area.
	create-time	Configures the installation time.
Configuring the Security Organization Code	**police-log set security-org-code**	Configures the security organization code.
Configuring the Collection System Type	**police-log set collection-type**	Configures the data collection system type.
Configuring the Data Transmission Source Identifier	**police-log set source-wacode**	Configures the data transmission source identifier.
Configuring the Data Transmission Destination Identifier	**police-log set destination-wacode**	Configures the data transmission destination identifier.
Configuring the FTP Server	**police-log set ftp server** *ip-address* **source** *ip-address*	Configures the FTP address and source interface.
Configuring the FTP Username and Password	**police-log set ftp username** *name* **password** *pass*	Configures the FTP username and password.
Configuring AP Information	**police-log add ap** { **service-name** | **service-code** | **service-type** | **apmac** | **longitude** | **latitude** | **address** }	Configures AP information.

2.4.1 Configuring Basic POLICE-LOG Function

Configuration Effect

- Interconnect with the MACC/ELOG, which can manage the current device.

Notes

- The address of the MACC/ELOG must be an integral uniform resource locator (URL).

Configuration Steps

Enabling POLICE-LOG Function

Command	**police-log enable**
Parameter Description	N/A
Defaults	This function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	Use this command to enable LOG_SERVER, to interconnect with the MACC/ELOG and send corresponding logs.

Setting MACC Address

Command	police-log set url *url*
Parameter Description	url: Specifies the integral MACC URL.
Defaults	No URL is configured by default.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure the URL of the MACC server. Note that the URL must be integral, and multiple sets of Web services may be deployed on the MACC server.

Setting Second MACC Address

Command	police-log set **second-url** *url*
Parameter Description	url: Specifies the second MACC URL.
Defaults	No URL is configured by default.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure the second MACC URL. Note that the URL must be integral, and multiple sets of Web services may be deployed on the MACC server.

Verification

- Run the **show police-log** command to check whether POLICE-LOG is enabled.

Command	**show police-log**
Parameter Description	N/A

Command Mode	Privileged EXEC mode and global configuration mode
Usage Guide	Use this command to check the running status of POLICE-LOG, that is, whether POLICE-LOG is enabled and whether POLICE-LOG is successfully interconnected with the MACC.
Configuration Example	1. Display the running status of POLICE-LOG. FS#show police-log config police log configuration >police log: enable >server url: https://192.168.25.184:443/specification >server url2: https://192.168.25.185:443/specification >auth type: define (1021999) >file compress: enable

Field	Description
police-log	Specifies the status of POLICE-LOG. This field can be set to **enable** or **disable**.
server url	Specifies the MACC/ELOG server URL.
server url2	Specifies the second MACC/ELOG server URL.
auth type	Specifies the authentication type.
file compress	Specifies the file compression switch. The value **enable** means compress and the value **disable** means not compress.

2.4.2 Configuring NAT-LOG Function

Configuration Effect

- Enable the gateway to audit NAT flows, so that the MACC can obtain information about the NAT flows.

Configuration Steps

Enabling NAT-LOG Function

Command	**nat-log police**
Parameter Description	N/A
Defaults	This function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show running | in nat-log** command to check whether NAT-LOG is enabled.

Command	**show running | in nat-log**
Parameter Description	N/A
Command Mode	Privileged EXEC mode and global configuration mode
Usage Guide	Use this command to check whether NAT-LOG is successfully enabled.
Configuration Example	1. Display the configuration status of NAT-LOG. FS#show running-config | in nat-log police nat-log police FS#

Field	Description
nat-log police on	**enable**: Specifies that the NAT log sending to the network monitoring platform is enabled. **disable**: Specifies that the NAT log sending to the network monitoring platform is enabled.
Other fields	N/A

2.4.3 Configuring General Log Function

Configuration Effect

- The gateway can audit the general online behavior data and send the data to the MACC for display and to the network monitoring platform.

Notes

- N/A

#if define(CONFIG_CONTENT_AUDIT) && (!defined(CONFIG_EG_CA_SMALL_MEMORY) || defined(CONFIG_EG_CA_URL_DB_FLASH))

Configuration Steps

Enabling General Log Sending to Network Monitoring Platform

Command	**content-audit write-plog {**im | mail | url | vid | web-bbs | web-mail | web-search**}**
Parameter Description	*im*: Enables the IM chat log sending to the network monitoring platform. *mail*: Enables the client mail log sending to the network monitoring platform. *url*: Enables the HTTP log sending to the network monitoring platform. !defined(CONFIG_EG_CA_NO_VID) && (!defined(CONFIG_EG_CA_SMALL_MEMORY) || defined(CONFIG_EG_CA_URL_DB_FLASH))

	vid: Enables the virtual identity audit log sending to the network monitoring platform. #endif *web-bbs*: Enables the Web BBS log sending to the network monitoring platform. *web-mail*: Enables the Web mail log sending to the network monitoring platform. *web-search*: Enables the Web search log sending to the network monitoring platform.
Defaults	This function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show content-audit plog config** command to check whether the general log sending to the network monitoring platform is enabled.

Command	**show content-audit plog config**
Parameter Description	N/A
Command Mode	Privileged EXEC mode/Global configuration mode
Usage Guide	Use this command to check whether the police parameters are successfully set for NAT logs.
Configuration Example	1. Check whether the police parameters are set to **enable** for NAT logs.

```
FS#show content-audit plog config
content-audit log send to police-log
-----------------------------------
    >im:                enable
    >vid:               enable
    >url:               enable
    >web search :       enable
    >web bbs :          enable
    >web mail:          enable
    >mail:              enable
```

Field	Description
im	**enable**: Specifies that the IM chat log function is enabled. **disable**: Specifies that the IM chat log function is disabled.
vid	**enable**: Specifies that the VID log function is enabled. **disable**: Specifies that the VID log function is disabled.

	url	**enable**: Specifies that the HTTP access log function is enabled. **disable**: Specifies that the HTTP access log function is disabled.
	web search	**enable**: Specifies that the Web search log function is enabled. **disable**: Specifies that the Web search log function is disabled.
	web bbs	**enable**: Specifies that the Web BBS log function is enabled. **disable**: Specifies that the Web BBS log function is disabled.
	web mail	**enable**: Specifies that the Web mail log function is enabled. **disable**: Specifies that the Web mail log function is disabled.
	mail	**enable**: Specifies that the client mail log function is enabled. **disable**: Specifies that the client mail log function is disabled.

2.4.4 Configuring an Interconnection Platform

Configuration Effect

- Configure a backend server interconnected with the network monitoring platform.

Notes

- N/A

Configuration Steps

Configuring an Interconnected Network Monitoring Platform

Command	**police-log set platform { elog | { *platform-type* [name *plat-name*] } }**
Parameter Description	**elog**: Indicates that the ELOG server is interconnected. If **elog** is selected, no additional parameter needs to be set. The ELOG server and third-party network monitoring platform are mutually exclusive. Only one of them can be selected. If this command is not configured, the ELOG server is interconnected by default. *platform-type*: Indicates the type of the third-party network monitoring platform. The value range can be queried using the **show plog platform** command. For example, **surfilter** indicates that a SURFILTER platform is interconnected while **myp** indicates that a Meiya Pico platform is interconnected. *plat-name*: Indicates the name of the network monitoring platform. If it is not set, the value is the same as that of *platform-type* by default.
Defaults	If this command is not configured, the ELOG server is interconnected by default. If *plat-name* is not set, the value of *plat-name* is the same as that of *platform-type*.

Command Mode	Global configuration mode
Usage Guide	After the configuration of this command is complete, the system enters the **config-plog-platform** command mode.

Configuring Parameters for the Network Monitoring Platform

Command	{ **data-gather** | **send-para** } *key-string value*
Parameter Description	**data-gather**: Configures parameters related to data collection. **send-para**: Configures parameters related to log sending. *key-string*: Indicates the name of a parameter. The name of the parameter is obtained using either of the following commands: **show plog para-list data-gather** *plat-name* **show plog para-list send-para** *palt-name* *value*: Indicates the parameter value.
Defaults	N/A
Command Mode	config-plog-platform mode
Usage Guide	An error is displayed if the configured name of a parameter falls beyond the list range of *key-string*.

Verification

- Run the **show plog config platform** command to display the list of configured network monitoring platforms.

Command	**show plog config platform**
Parameter Description	N/A
Command Mode	Privileged EXEC mode and global configuration mode
Usage Guide	N/A
Configuration Example	FS(config)#show plog config platform Platform-type Platform-name ========== surfilter Fuzhou-police
Prompt	N/A

- Run the **show plog config { data-gather | send-para } platform** *plat-name* command to display the configuration information of the network monitoring platform.

Command	**show plog config { data-gather | send-para } platform** *plat-name*
Parameter Description	*plat-name*: Indicates the name of the network monitoring platform.
Command Mode	Privileged EXEC mode and global configuration mode
Usage Guide	Parameters are listed regardless of whether they are configured for the network monitoring platform.
Configuration Example	FS(config)#show plog config data-gather platform renzixing DATA-GATHER: security-org-code: collection-type: source-wacode: destination-wacode: org-name: org-address: org-person: org-tel: org-mail: FS(config)#show plog config send-para platform renzixing SEND-CONFIG: ftp-server-ip:112.112.30.32 ftp-username:user ftp-password:pass
Prompt	N/A

Configuration Example

N/A

2.4.5 Configuring Site Information

Configuration Effect

- The gateway can obtain site data and send it to a third-party system.

Notes

- N/A

Configuration Steps

Configuring a Site

Command	**police-log-netsite** *index*
Parameter Description	*Index*: Specifies the site index.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	After the configuration is complete, the system enters the **config-plog-netsite** command mode.

Configuring the Network Monitoring Platform to Which the Site Belongs

Command	**platform** *plat-name*
Parameter Description	*plat-name*: Indicates the network monitoring platform to which the site belongs.
Defaults	N/A
Command Mode	config-plog-netsite mode
Usage Guide	This command can be executed three times at most for the same site. The three network monitoring platforms to which a site can belong must share the same type. Otherwise, an error will arise.

Configuring Site Parameters

Command	*key-string value*
Parameter Description	*key-string*: Indicates the name of a site parameter. The name of the site parameter can be obtained by using the **show plog para-list netsite** *palt-name* command. *Value*: Indicates the parameter value.
Defaults	N/A
Command Mode	config-plog-netsite mode
Usage Guide	An error is displayed if the configured parameter name is invalid.

Verification

- Run the **show plog config netsite** [*netsite-id* | **platform** *plat-name*] command to display the configuration information of the specified network monitoring platform.

Command	**show plog config netsite** [*netsite-id* | **platform** *plat-name*]
Parameter Description	*netsite-id*: Specifies the site ID.
	plat-name: Specifies the name of the network monitoring platform.
Command Mode	Privileged EXEC mode and global configuration mode
Usage Guide	1. If no parameter is configured, a list of all Internet access sites that belong to related network monitoring platforms is displayed.

	2. If *netsite-id* is specified, information about the specified site is displayed. 3. If *plat-name* is specified, information about sites that belong to this network monitoring platform is displayed.
Configuration Example	FS(config)#show plog config netsite 1 netsite:1, platform:renzixing service-code: service-type: address: longitude: latitude: business-nature: status: principal: principal-cert-type: principal-cert-code: principal-phone: start-time: end-time: producer-type: producer-code: province-code: city-code: area-code: create-time:
Prompt	N/A

Configuration Example

N/A

Common Errors

N/A

2.4.6 Configuring a Security Organization Code

Configuration Effects

- Configure a security organization code.

Notes

- N/A

Steps

Configuring a Security Organization Code

Command	**police-log set security-org-code** *code*
Parameter Description	code: Specifies the organization code.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show run** command to display the security organization code.

Command	**show run**
Parameter Description	N/A
Defaults	N/A
Command Mode	Privileged EXEC mode/Global configuration mode
Usage Guide	N/A

Configuration Example

N/A

Common Errors

N/A

2.4.7 Configuring a Collection System Type

Configuration Effects

- Configure a collection system type.

Notes

- -

Steps

Configuring a Collection System Type

Command	**police-log set collection-type** *type*
Parameter Description	*type*: Configures the collection system type.
Defaults	N/A
Command Mode	Global configuration mode

Usage Guide	N/A

Verification

- Run the **show run** command to display the collection system type.

Command	**show run**
Parameter Description	N/A
Defaults	N/A
Command Mode	Privileged EXEC mode/Global configuration mode
Usage Guide	N/A

Configuration Example

N/A

Common Errors

N/A

2.4.8 Configuring a Source Code for Data Transmission

Configuration Effects

- Configure a source code for data transmission.

Notes

- N/A

Steps

Configuring a Source Code for Data Transmission

Command	**police-log set source-wacode** *code*
Parameter Description	*code*: Configures the source code.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show run** command to display the source code.

Command	**show run**
Parameter	N/A

Description	
Defaults	N/A
Command Mode	Privileged EXEC mode/Global configuration mode
Usage Guide	N/A

Configuration Example

N/A

Common Errors

N/A

2.4.9 Configuring a Destination Code for Data Transmission

Configuration Effects

- Configure a destination code for data transmission.

Notes

- N/A

Steps

Configuring a Destination Code for Data Transmission

Command	**police-log set destination-wacode** *code*
Parameter Description	*code*: Configures the destination code.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show run** command to display the destination code.

Command	**show run**
Parameter Description	N/A
Defaults	N/A
Command Mode	Privileged EXEC mode/Global configuration mode
Usage Guide	N/A

Configuration Example

N/A

Common Errors

N/A

2.4.10 Configuring a Security Organization Name

Configuration Effects

- Configure a security organization name.

Notes

- N/A

Steps

Configuring a Security Organization Code

Command	**police-log set org-name** *name*
Parameter Description	*name*: Specifies a security organization name.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show run** command to display the security organization name.

Command	**show run**
Parameter Description	N/A
Defaults	N/A
Command Mode	Privileged EXEC mode/Global configuration mode
Usage Guide	N/A

Configuration Example

N/A

Common Errors

N/A

2.4.11 Configuring a Security Organization Address

Configuration Effects

- Configure a security organization address.

Notes

- N/A

Steps

Configuring a Security Organization Address

Command	**police-log set org-address** *address*
Parameter Description	*address:* Specifies the security organization address.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show run** command to display the security organization address.

Command	**show run**
Parameter Description	N/A
Defaults	N/A
Command Mode	Privileged EXEC mode/Global configuration mode
Usage Guide	N/A

Configuration Example

N/A

Common Errors

N/A

2.4.12 Configuring a Security Organization Contact

Configuration Effects

- Configure a security organization contact.

Notes

- N/A

Steps

Configuring a Security Organization Contact

Command	**police-log set org-person** *person*
Parameter Description	*person*: Specifies a contact person.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show run** command to display the contact person.

Command	**show run**
Parameter Description	N/A
Defaults	N/A
Command Mode	Privileged EXEC mode/Global configuration mode
Usage Guide	N/A

Configuration Example

N/A

Common Errors

N/A

2.4.13 Configuring a Security Organization Phone Number

Configuration Effects

- Configuring a security organization phone number.

Notes

- N/A

Steps

Configuring a Security Organization Phone Number

Command	**police-log set org-tel** *tel*
Parameter	*tel*: Specifies a security organization phone number.

Description	
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show run** command to display the mobile number.

Command	**show run**
Parameter Description	N/A
Defaults	N/A
Command Mode	Privileged EXEC mode/Global configuration mode
Usage Guide	N/A

Configuration Example

N/A

Common Errors

N/A

2.4.14 Configuring a Security Organization Mail

Configuration Effects

- Configure a security organization mail.

Notes

- N/A

Steps

Configuring a Security Organization Mail

Command	**police-log set org-mail** *mail*
Parameter Description	*mail*: Specifies a security organization mail.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show run** command to display the security organization mail.

Command	**show run**
Parameter Description	N/A
Defaults	N/A
Command Mode	Privileged EXEC mode/Global configuration mode
Usage Guide	N/A

Configuration Example

N/A

Common Errors

N/A

2.4.15 Configuring an FTP Server

Configuration Effects

- Configure an FTP server.

Notes

- N/A

Steps

Configuring an FTP server

Command	**police-log set ftp server** *ip-address* **source** *interface-name*
Parameter Description	*Ip-address*: Specifies an IP address. *interface-name*: Specifies an interface.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show run** command to display the FTP server.

Command	**show run**
Parameter Description	N/A

Defaults	N/A
Command Mode	Privileged EXEC mode/Global configuration mode
Usage Guide	N/A

Configuration Example

N/A

Common Errors

N/A

2.4.16 Configuring an FTP Username and Password

Configuration Effects

- Configure an FTP username and password.

Notes

- -

Steps

Configuring an FTP Username and Password

Command	**police-log set ftp username** *user* **password** *pass*
Parameter Description	*user*: Specifies an FTP username. *pass*: Specifies an FTP password.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show run** command to display the FTP username and password.

Command	**show run**
Parameter Description	N/A
Defaults	N/A
Command Mode	Privileged EXEC mode/Global configuration mode
Usage Guide	N/A

Configuration Example

N/A

Common Errors

N/A

2.4.17 Configuring AP Information

Configuration Effect

- The gateway can generate AP data based on configured AP information and sends the generated AP data logs to the network monitoring platform.

Notes

- N/A

Configuration Steps

Configuring an AP

Command	**police-log-ap** *index*
Parameter Description	index: Specifies the index of an AP.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	After the configuration is complete, the system enters the **config-plog-ap** command mode.

Configuring a Site to Which the AP Belongs

Command	**service-code** *code-value*
Parameter Description	code-value: Specifies the code of the Internet access service site.
Defaults	N/A
Command Mode	config-plog-ap mode
Usage Guide	This command must be configured before other parameters are set. Otherwise, an error will occur. One AP can belong only to one site.

Configuring Site Parameters

Command	*key-string value*
Parameter Description	*key-string*: Indicates the name of an AP parameter. The name of the AP parameter can be obtained by using the **show plog para-list ap { platform** *plat-name* **/netsite** *id* **}** command. *Value*: Indicates the parameter value.
Defaults	N/A

Command Mode	config-plog-ap mode
Usage Guide	The service code of the site to which the AP belongs must be configured first. Otherwise, an exception will arise.

Verification

- Run the **show plog config ap** [*ap-id* | **netsite** *netsite-id* | **platform** *plat-name*] command to display the configuration information of the AP.

Command	**show plog config ap** [*ap-id* | **netsite** *netsite-id* | **platform** *plat-name*]
Parameter Description	*ap-id*: Specifies the ID of the AP. *netsite-id*: Specifies the site ID.
	plat-name: Specifies the name of the network monitoring platform.
Command Mode	Privileged EXEC mode and global configuration mode
Usage Guide	1. If no parameter is configured, information about all APs is displayed. 2. If *ap-id* is specified, information about the specified AP is displayed. 3. If *netsite-id* is specified, information about APs belonging to the specified site is displayed. 4. If *plat-name* is specified, information about APs under the management of the specified network monitoring platform is displayed.
Configuration Example	show plog config ap ap:1, netsite:1, platform:renzixing service-code:12345678901234 ap-mac:00d0.f8fb.1122 ap-name:ABC ap-type: ap-floor:7 create-time:2018-9-18 ap:2, netsite:1, platform:renzixing service-code:12345678901234 ap-mac:00d0.f8fb.1133 ap-name:DEF ap-type: ap-floor:8 create-time:2018-9-18
Prompt	N/A

2.5 Monitoring

Displaying

Description	Command
Displays the running status.	**show police-log status**
Displays the platform.	**show plog platform**
Displays the parameters supported by the current platform.	**show plog para-list**
Displays the configuration.	**show plog config**

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs the POLICE-LOG switch.	**debug police-log**

3 Configuring LOG-POLICY

3.1 Overview

LOG-POLICY can provide refined log control and specify the log type based on the user name, IP address, or IP range. In the past, all logs are generated in the same way, and some logs may fail to meet user requirements.

3.2 Applications

Application	Description
LOG-POLICY	Describe basic scenarios and functions of LOG-POLICY.

3.2.1 Typical Application Scenarios

Scenario

Specify the type of logs to be reported by users.

Deployment

Customize a log policy based on the user name, IP address, or IP range.

3.3 Features

3.3.1 LOG-POLICY

Set the log type to be reported by a user or an IP address.

Working Principle

LOG-POLICY limits the log type reported by a user or an IP address based on specific rules.

Related Configuration

Run the **log-policy** command to create a log policy.

Run the **log-policy-relate** command to set the object associated with the log policy.

Configure rule parameters to determine the log type to be reported.

Change the priorities of two log policies.

3.4 Configuration

3.4.1 Configuring a Log Policy

Configuration Effect

- Create a log policy object.

Notes

- A policy configured earlier takes effect prior to a policy configured later.

Configuration Steps

Configuring a Log Policy

- Mandatory.

Verification

Run the **show log-policy** command to display the configuration.

Related Commands

Configuring a Log Policy

Command	**log-policy** *policy-name* { **netlog** | **82log** | **none** }
Parameter Description	*policy-name*: Indicates the log policy name.
Command Mode	Global configuration mode
Usage Guide	Generate a log policy. 1. Log policies must have unique names. 2. To delete the log policy, run the **no log-policy** *policy-name* command in global configuration mode.

Configuration Example

Configuring a Log Policy

Configuration Steps	● Run the following commands.
	FS# configure terminal FS(config)# log-policy auth 82log FS(config)# end
Verification	● Run the **show log-policy** command to display the configuration.
	FS# show log-policy log-policy auth 82log

Common Errors

- The regular expression does not meet syntax requirements.
- The number of policies exceeds the limit of 1,000.
- The policy name exceeds the maximum length of 64 bytes.

3.4.2 Setting the Object Associated with a Log Policy

Configuration Effect

- Set the object associated with a log policy.

Notes

- Each IP-based log policy can associate with only one object.
- Each username-based log policy can associate with a maximum of 10 user objects.
- A log policy based on user configuration with a bound MAC address can be used only at layer 2.
- A log policy based on user configuration with a bound MAC address does not support authentication logs in SAM, SMP, and ESS authentication scenarios.

Configuration Steps

Configuring a Log Policy

- Mandatory.

Verification

Run the **show log-policy** command to display the configuration.

Related Commands

Configuring a Log Policy

Command	**log-policy-relate relate policyname** policy-name { **ip-host** *ip-address* | **ip-subnet** *subnet-address subnet-mask* | **ip-range** *ip-address-begin ip-address-end* | **subscriber** *user-name* | **auth-subscribe** *user-name* }
Parameter Description	*policy-name*: Indicates the log policy name. *ip-address*: Indicates the IP address. *subnet-address*: Indicates the subnet address. subnet-mask: Indicates the subnet mask. ip-address-begin: Indicates the start IP address. ip-address-end: Indicates the end IP address. *user-name: Indicates the user name.*
Command Mode	Global configuration mode
Usage Guide	Set the object associated with a log policy. 1. The log policy must exist. 2: To delete the log policy, run the following command in global configuration mode: **no log-policy-relate relate policyname** *policy-name* { **ip-host** *ip-address* | **ip-subnet** *subnet-address subnet-mask* | **ip-range** *ip-address-start ip-address-end* | **subscriber** *user-name* | **auth-subscribe** *user-name* }
	A log policy based on user configuration with a bound MAC address can be used only at layer 2 and does not support authentication logs in SAM, SMP, and ESS authentication scenarios. When the user management module or marketing authentication module is restarting, no authentication log is available.

Configuration Example

Configuring a Log Policy

Configuration Steps	● Configuration example
	FS# configure terminal FS(config)# log-policy-relate relate policyname subnet ip-subnet 192.168.5.0 255.255.255.0 FS(config)# log-policy-relate relate policyname range ip-range 192.168.3.1 192.168.5.1 FS(config)# log-policy-relate relate policyname ip ip-host 192.168.3.11 FS(config)# log-policy-relate relate policyname sub-any subscriber any FS(config)# log-policy-relate relate policyname auth auth-subscribe any FS(config)# end
Verification	● Run the **show log-policy** command to display the configuration.
	FS# show log-policy log-policy subnet none log-policy-relate relate policyname subnet ip-subnet 192.168.5.0 255.255.255.0 log-policy range 82log log-policy-relate relate policyname range ip-range 192.168.3.1 192.168.5.1 log-policy ip none log-policy-relate relate policyname ip ip-host 192.168.3.11 log-policy auth netlog log-policy-relate relate policyname auth auth-subscribe any log-policy sub-any netlog log-policy-relate relate policyname sub-any subscriber any

Common Errors

- The regular expression does not meet syntax requirements.
- The policy name exceeds the maximum length of 64 bytes.
- The user name exceeds the maximum length of 128 bytes.
- When a log policy is configured based on the IP range, the start IP address is greater than the end IP address.
- The user name or IP address has been used.

3.4.3 Changing the Priorities of Two Log Policies

Configuration Effect

- Change the priorities of two log policies.

Notes

- The two log policies must be in sequence in the command.

Configuration Steps

Changing the Priorities of Two Log Policies

- Mandatory.

Verification

Run the **show log-policy** command to display the configuration.

Related Commands

Changing the Priorities of Two Log Policies

Command	**log-policy-config priority-swap** *policy-name1 policy-name2*
Parameter Description	*policy-name*1: Indicates the log policy name. *policy-name*2: Indicates the log policy name.
Command Mode	Global configuration mode
Usage Guide	Change the priorities of two log policies. 1. The two policies must exist. 2: The two policies must be in sequence in the command.

Configuration Example

Changing the Priorities of Two Log Policies

Configuration Steps	● Configuration example
	FS#show log-policy log-policy subnet none log-policy-relate relate policyname subnet ip-subnet 192.168.5.0 255.255.255.0 log-policy range 82log log-policy-relate relate policyname range ip-range 192.168.3.1 192.168.5.1 log-policy ip none log-policy-relate relate policyname ip ip-host 192.168.3.11 log-policy auth netlog log-policy-relate relate policyname auth auth-subscribe any log-policy sub-any netlog log-policy-relate relate policyname sub-any subscriber any FS(config)# log-policy-config priority-swap subnet range FS(config)# end
Verification	● Run the **show log-policy** command to display the configuration.
	FS#show log-policy log-policy range 82log log-policy-relate relate policyname range ip-range 192.168.3.1 192.168.5.1 log-policy subnet none log-policy-relate relate policyname subnet ip-subnet 192.168.5.0 255.255.255.0 log-policy ip none

	log-policy-relate relate policyname ip ip-host 192.168.3.11 log-policy auth netlog log-policy-relate relate policyname auth auth-subscribe any log-policy sub-any netlog log-policy-relate relate policyname sub-any subscriber any

Common Errors

- The regular expression does not meet syntax requirements.
- Either log policy does not exist.
- The two log policies are not in sequence in the command.

3.5 Monitoring

Clearing

Description	Command
Clears all log policies.	**clear log-policy**

Displaying

Description	Command
Displays log policy information.	**show log-policy** [**policyname** *policy-name*]

4 Configuring SNMP

4.1 Overview

Simple Network Management Protocol (SNMP) became a network management standard RFC1157 in August 1988. At present, because many vendors support SNMP, SNMP has in fact become a network management standard and is applicable to the environment where systems of multiple vendors are interconnected. By using SNMP, the network administrator can implement basic functions such as information query for network nodes, network configuration, fault locating, capacity planning, and network monitoring and management.

➘ SNMP Versions

Currently, the following SNMP versions are supported:

- SNMPv1: The first official version of SNMP, which is defined in RFC1157.
- SNMPv2C: Community-based SNMPv2 management architecture, which is defined in RFC1901.
- SNMPv3: SNMPv3 provides the following security features by identifying and encrypting data.

5. Ensuring that data is not tampered during transmission.
6. Ensuring that data is transmitted from legal data sources.
7. Encrypting packets and ensuring data confidentiality.

Protocols and Standards

- RFC 1157, Simple Network Management Protocol (SNMP)
- RFC 1901, Introduction to Community-based SNMPv2
- RFC 2578, Structure of Management Information Version 2 (SMIv2)
- RFC 2579, Textual Conventions for SMIv2
- RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
- RFC 3412, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 3413, Simple Network Management Protocol (SNMP) Applications
- RFC 3414, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
- RFC 3415, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
- RFC 3416, Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
- RFC 3417, Transport Mappings for the Simple Network Management Protocol (SNMP)
- RFC 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
- RFC 3419, Textual Conventions for Transport Addresses

4.2 Applications

Application	Description
Managing Network Devices Based on	Network devices are managed and monitored based on SNMP.

SNMP	

4.2.1 Managing Network Devices Based on SNMP

Scenario

Take the following figure as an example. Network device A is managed and monitored based on SNMP network manager.

Figure 4-1

Remarks	A is a network device that needs to be managed. PC is a network management station.

Deployment

The network management station is connected to the managed network devices. On the network management station, users access the Management Information Base (MIB) on the network devices through the SNMP network manager and receive messages actively sent by the network devices to manage and monitor the network devices.

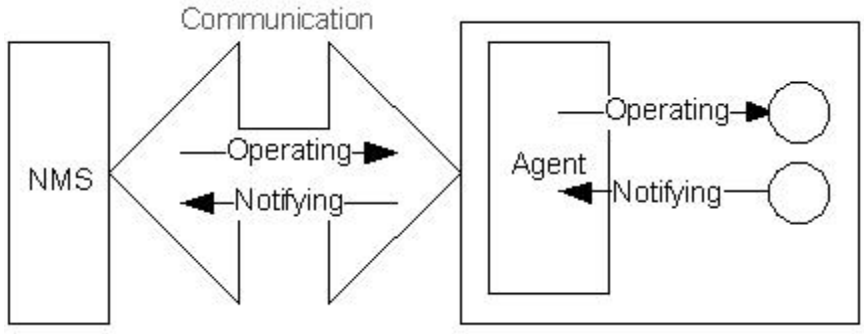
4.3 Features

Basic Concepts

SNMP is an application layer protocol that works in C/S mode. It consists of three parts:

- SNMP network manager
- SNMP agent
- MIB

Figure 4-2 shows the relationship between the network management system (NMS) and the network management agent.



↘ SNMP Network Manager

The SNMP network manager is a system that controls and monitors the network based on SNMP and is also called the NMS.

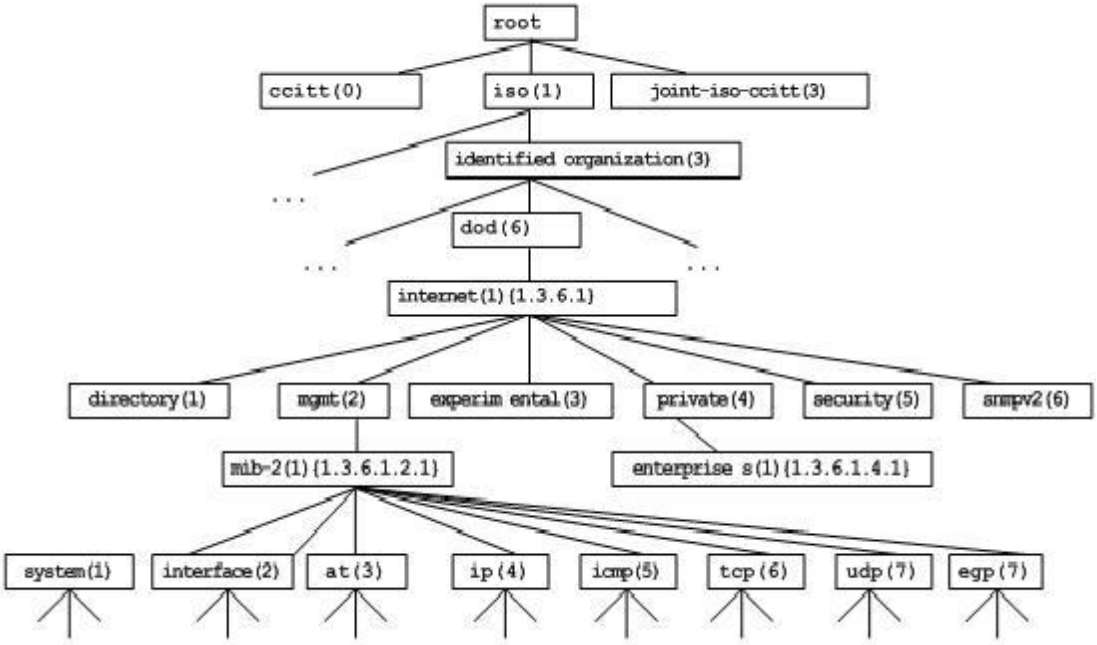
SNMP Agent

The SNMP agent (hereinafter referred to as the agent) is software running on the managed devices. It is responsible for receiving, processing, and responding to monitoring and control packets from the NMS. The agent may also actively send messages to the NMS.

MIB

The MIB is a virtual network management information base. The managed network devices contain lots of information. To uniquely identify a specific management unit among SNMP packets, the MIB adopts the tree hierarchical structure. Nodes in the tree indicate specific management units. A string of digits may be used to uniquely identify a management unit system among network devices. The MIB is a collection of unit identifiers of network devices.

Figure 4-3 Tree Hierarchical Structure



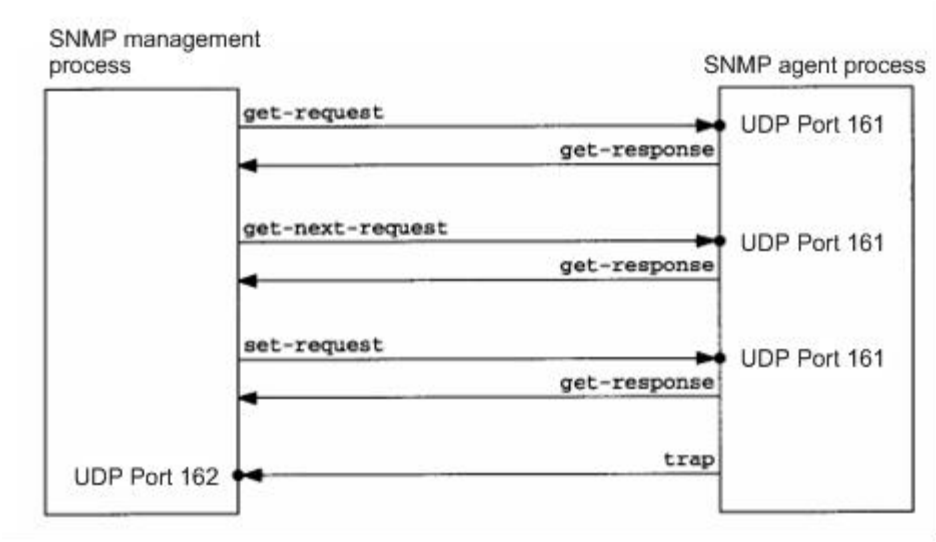
Operation Types

Six operation types are defined for information exchange between the NMS and the agent based on SNMP:

- Get-request: The NMS extracts one or more parameter values from the agent.
- Get-next-request: The NMS extracts the parameter value next to one or more parameters from the agent.
- Get-bulk: The NMS extracts a batch of parameter values from the agent.
- Set-request: The NMS sets one or more parameter values of the agent.
- Get-response: The agent returns one or more parameter values, which are the operations in response to the three operations performed by the agent on the NMS.
- Trap: The agent actively sends a message to notify the NMS of something that happens.

The first four packets are sent by the NMS to the agent and the last two packets are sent by the agent to the NMS. (Note: SNMPv1 does not support the Get-bulk operation.) Figure 2-4 describes the operations.

Figure 4-4 SNMP Packet Types



The three operations performed by the NMS on the agent and the response operations of the agent are based on UDP port 161. The trap operation performed by the agent is based on UDP port 162.

Overview

Feature	Description
Basic SNMP Functions	The SNMP agent is configured on network devices to implement basic functions such as information query for network nodes, network configuration, fault locating, and capacity planning.
SNMPv1 and SNMPv2C	SNMPv1 and SNMPv2C adopt the community-based security architecture, including authentication name and access permission.
SNMPv3	SNMPv3 redefines the SNMP architecture, namely, it enhances security functions, including the security model based on users and access control model based on views. The SNMPv3 architecture already includes all functions of SNMPv1 and SNMPv2C.

4.3.1 Basic SNMP Functions

Working Principle

Working Process

SNMP protocol interaction is response interaction (for exchange of packets, see Figure 2-4). The NMS actively sends requests to the agent, including Get-request, Get-next-request, Get-bulk, and Set-request. The agent receives the requests, completes operations, and returns a Get-response. Sometimes, the agent actively sends a trap message and an Inform message to the NMS. The NMS does not need to respond to the trap message but needs to return an Inform-response to the agent. Otherwise, the agent re-sends the Inform message.

Related Configuration

Shielding or Disabling the SNMP Agent

By default, the SNMP function is enabled.

The **no snmp-server** command is used to disable the SNMP agent.

The **no enable service snmp-agent** command is used to directly disable all SNMP services.

Setting Basic SNMP Parameters

By default, the system contact mode, system location, and device Network Element (NE) information are empty. The default serial number is 60FF60, the default maximum packet length is 1,572 bytes, and the default UDP port ID of the SNMP service is 161.

The **snmp-server contact** command is used to configure or delete the system contact mode.

The **snmp-server location** command is used to configure or delete the system location.

The **snmp-server chassis-id** command is used to configure the system serial number or restore the default value.

The **snmp-server packetsize** command is used to configure the maximum packet length of the agent or restore the default value.

The **snmp-server net-id** command is used to configure or delete the device NE information.

The **snmp-server udp-port** command is used to set the UDP port ID of the SNMP service or restore the default value.

Configuring the SNMP Host Address

By default, no SNMP host is configured.

The **snmp-server host** command is used to configure the NMS host address to which the agent actively sends messages or to delete the specified SNMP host address. In the messages sent to the host, the SNMP version, receiving port, authentication name, or user can be bound. This command is used with the **snmp-server enable traps** command to actively send trap messages to the NMS.

Setting Trap Message Parameters

By default, SNMP is not allowed to actively send a trap message to the NMS, the function of sending a Link Trap message on an interface is enabled, the function of sending a system reboot trap message is disabled, and a trap message does not carry any private field.

By default, the IP address of the interface where SNMP packets are sent is used as the source address.

By default, the length of a trap message queue is 10 and the interval for sending a trap message is 30s.

The **snmp-server enable traps** command is used to enable or disable the agent to actively send a trap message to the NMS.

The **snmp trap link-status** command is used to enable or disable the function of sending a Link Trap message on an interface.

The **snmp-server trap-source** command is used to specify the source address for sending messages or to restore the default value.

The **snmp-server queue-length** command is used to set the length of a trap message queue or to restore the default value.

The **snmp-server trap-timeout** command is used to set the interval for sending a trap message or to restore the default value.

The **snmp-server trap-format private** command is used to set or disable the function of carrying private fields in a trap message when the message is sent.

The **snmp-server system-shutdown** command is used to enable or disable the function of sending a system reboot trap message.

Setting the SNMP Attack Protection and Detection Function

By default, the SNMP attack protection and detection function is disabled.

The **snmp-server authentication attempt** *times* **exceed** { **lock** | **lock-time** *minutes* | **unlock** } command is used to set and enable the attack protection and detection function.

Setting Password Dictionary Check for Communities and Users

By default, password dictionary check for communities and users is disabled.

The **snmp-server enable secret-dictionary-check** command is used to enable password dictionary check for SNMP communities and users. This command is used with the **password policy** command.

4.3.2 SNMPv1 and SNMPv2C

SNMPv1 and SNMPv2C adopt the community-based security architecture. The administrator who can perform operations on the MIB of the agent is limited by defining the host address and authentication name (community string).

Working Principle

SNMPv1 and SNMPv2 determine whether the administrator has the right to use MIB objects by using the authentication name. The authentication name of the NMS must be the same as an authentication name defined in devices.

SNMPv2C adds the Get-bulk operation mechanism and can return more detailed error message types to the management workstation. The Get-bulk operation is performed to obtain all information from a table or obtain lots of data at a time, so as to reduce the number of request responses. The enhanced error handling capabilities of SNMPv2C include extension of error codes to differentiate error types. In SNMPv1, however, only one error code is provided for errors. Now, errors can be differentiated based on error codes. Because management workstations supporting SNMPv1 and SNMPv2C may exist on the network, the SNMP agent must be able to identify SNMPv1 and SNMPv2C packets and return packets of the corresponding versions.

➘ Security

One authentication name has the following attributes:

- Read-only: Provides the read permission of all MIB variables for authorized management workstations.
- Read-write: Provide the read/write permission of all MIB variables for authorized management workstations.

Related Configuration

➘ Setting Authentication Names and Access Permissions

The default access permission of all authentication names is read-only.

The **snmp-server community** command is used to configure or delete an authentication name and access permission.

This command is the first important command for enabling the SNMP agent function. It specifies community attributes and NMS scope where access to the MIB is allowed.

4.3.3 SNMPv3

SNMPv3 redefines the SNMP architecture and includes functions of SNMPv1 and SNMPv2 into the SNMPv3 system.

Working Principle

The NMS and SNMP agent are SNMP entities. In the SNMPv3 architecture, SNMP entities consist of the SNMP engine and SNMP applications. The SNMP engine is used to send and receive messages, identify and encrypt information, and control access to managed objects. SNMP applications refer to internal applications of SNMP, which work by using the services provided by the SNMP engine.

SNMPv3v determines whether a user has the right to use MIB objects by using the User-based Security Model (USM). The security level of the NMS user must be the same as that of an SNMP user defined in devices so as to manage devices.

SNMPv3 requires the NMS to obtain the SNMP agent engine IDs on devices when the NMS manages devices. SNMPv3 defines the discover and report operation mechanisms. When the NMS does not know agent engine IDs, the NMS may first send a discover message

to the agent and the agent returns a report message carrying an engine ID. Later, management operations between the NMS and the agent must carry the engine ID.

Security

- SNMPv3 determines the data security mechanism based on the security model and security level. At present, security models include: SNMPv1, SNMPv2C, and SNMPv3. SNMPv3 includes SNMPv1 and SNMPv2C into the security model.

SNMPv1 and SNMPv2C Security Models and Security Levels

Security Model	Security Level	Authentication	Encryption	Description
SNMPv1	noAuthNoPriv	Authentication name	N/A	Data validity is confirmed through authentication name.
SNMPv2c	noAuthNoPriv	Authentication name	N/A	Data validity is confirmed through authentication name.

SNMPv3 Security Model and Security Level

Security Model	Security Level	Authentication	Encryption	Description
SNMPv3	noAuthNoPriv	User name.	N/A	Data validity is confirmed through user name.
SNMPv3	authNoPriv	MD5 or SHA	N/A	The data authentication mechanism based on HMAC-MD5 or HMAC-SHA is provided.
SNMPv3	authPriv	MD5 or SHA	DES	The data authentication mechanism based on HMAC-MD5 or HMAC-SHA and data encryption mechanism based on CBC-DES are provided.

Engine ID

An engine ID is used to uniquely identify an SNMP engine. Because each SNMP entity includes only one SNMP engine, one SNMP engine uniquely identifies an SNMP entity in a management domain. Therefore, the SNMPv3 agent as an entity must has a unique engine ID, that is, SnmpEngineID.

An engine ID is an octet string that consists of 5 to 32 bytes. RFC3411 defines the format of an engine ID:

- The first four bytes indicate the private enterprise ID (allocated by IANA) of a vendor, which is expressed in hexadecimal.
- The fifth byte indicates remaining bytes:
- 0: Reserved.
- 1: The later four bytes indicate an IPv4 address.
- 3: The later six bytes indicate a MAC address.
- 4: Text consisting of 27 bytes, which is defined by the vendor.
- 5: Hexadecimal value consisting of 27 bytes, which is defined by the vendor.
- 6-127: Reserved.

- 128-255: Formats specified by the vendor.

Related Configuration

Configuring an MIB View and a Group

By default, one view is configured and all MIB objects can be accessed.

By default, no user group is configured.

The **snmp-server view** command is used to configure or delete a view and the **snmp-server group** command is used to configure or delete a user group.

One or more instructions can be configured to specify different community names so that network devices can be managed by NMSs of different permissions.

Configuring an SNMP User

By default, no user is configured.

The **snmp-server user** command is used to configure or delete a user.

The NMS can communicate with the agent by using only legal users.

An SNMPv3 user can specify the security level (whether authentication and encryption are required), authentication algorithm (MD5 or SHA), authentication password, encryption password (only DES is available currently), and encryption password.

4.4 Configuration

Configuration	Description and Command	
Configuring Basic SNMP Functions	(Mandatory) It is used to enable users to access the agent through the NMS.	
	enable service snmp-agent	Enables the agent function.
	snmp-server community	Sets an authentication name and access permission.
	snmp-server user	Configures an SNMP user.
	snmp-server view	Configures an SNMP view.
	snmp-server group	Configures an SNMP user group.
	snmp-server authentication	Configures the SNMP attack protection and detection function.
	snmp-server enable secret-dictionary-check	Configures password dictionary check for communities and users.
Enabling the Trap Function	(Optional) It is used to enable the agent to actively send a trap message to the NMS.	
	snmp-server host	Configures the NMS host address.
	snmp-server enable traps	Enables the agent to actively send a trap message to the NMS.
	snmp trap link-status	Enables the function of sending a Link Trap message on an interface.

Configuration	Description and Command	
	snmp-server system-shutdown	Enables the function of sending a system reboot trap message.
	snmp-server trap-source	Specifies the source address for sending a trap message.
	snmp-server trap-format private	Enables a trap message to carry private fields when the message is sent.
Shielding the Agent Function	(Optional) It is used to shield the agent function when the agent service is not required.	
	no snmp-server	Shields the agent function.
Setting SNMP Control Parameters	(Optional) It is used to set or modify SNMP control parameters.	
	snmp-server contact	Sets the device contact mode.
	snmp-server location	Sets the device location.

4.4.1 Configuring Basic SNMP Functions

Configuration Effect

Enable users to access the agent through the NMS.

Notes

- By default, no authentication name is set on network devices and SNMPv1 or SNMPv2C cannot be used to access the MIB of network devices. When an authentication name is set, if no access permission is specified, the default access permission is read-only.

Configuration Steps

Configuring an SNMP View

- Optional
- An SNMP view needs to be configured when the View-based Access Control Model (VACM) is used.

Configuring an SNMP User Group

- Optional
- An SNMP user group needs to be configured when the VACM is used.

Configuring an Authentication Name and Access Permission

- Mandatory
- An authentication name must be set on the agent when SNMPv1 and SNMPv2C are used to manage network devices.

Configuring an SNMP User

- Mandatory
- A user must be set when SNMPv3 is used to manage network devices.

Enabling the Agent Function

- Optional
- By default, the agent function is enabled. When the agent function needs to be enabled again after it is disabled, this command must be used.

Enabling the SNMP Attack Protection and Detection Function

- Optional
- By default, the SNMP attack protection and detection function is disabled. When malicious attacks need to be prevented, the configuration item must be used on the agent.

Setting Password Dictionary Check for Communities and Users

- Optional
- By default, password dictionary check is not performed for communities and users. If community names and user names are too simple and are easily cracked, enable password dictionary check for communities and users. The configuration must be used with the **password policy** command.

Setting the SNMP Logging Function to Record the Get, Get-Next, and Set Operations Performed by the NMS on the SNMP Agent

- Optional
- The SNMP logging function is used to record the Get, Get-Next, and Set Operations performed by the NMS on the SNMP agent. When the Get and Get-Next operations are performed, the agent records the IP address of the NMS user, operation type, and OID of the operation node. When the Set operation is performed, the agent records the IP address of the NMS user, operation type, OID of the operation node, and set value. These logs are sent to the information center of devices. The level of these logs is informational, that is, the logs are used as prompt information of devices.

Verification

Run the **show snmp** command to check the SNMP function on devices.

Related Commands

Configuring an SNMP View

Command	**snmp-server view** *view-name oid-tree* { **include** | **exclude** }
Parameter Description	*view-name*: View name *oid-tree*: MIB objects associated with a view, which are displayed as an MIB subtree. **include:** Indicates that the MIB object subtree is included in the view. **exclude:** Indicates that the MIB object subtree is not included in the view.
Command Mode	Global configuration mode
Usage Guide	Specify a view name and use it for view-based management.

Configuring an SNMP User Group

Command	**snmp-server group** *groupname* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } } [**read** *readview*] [**write** *writeview*] [**access** { **ipv6**

	ipv6-aclname | *aclnum* | *aclname* }]
Parameter Description	**v1** | **v2c** |**v3:** Specifies the SNMP version. **auth:** Messages sent by users in the group need to be verified but data confidentiality is not required. This configuration is valid for SNMPv3 only. **noauth:** Messages sent by users in the group do not need to be verified and data confidentiality is not required. This configuration is valid for SNMPv3 only. **priv:** Messages sent by users in the group need to be verified and confidentiality of transmitted data is required. This configuration is valid for SNMPv3 only. *readview*: Associates one read-only view. *writeview*: Associates one read/write view. *aclnum*: ACL number. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *aclname*: ACL name. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *ipv6-aclname*: IPv6 access list name, which specifies the IPv6 addresses that are permitted to access the MIB.
Command Mode	Global configuration mode
Usage Guide	Associate certain users with a group and associate the group with a view. Users in a group have the same access permission. In this way, you can determine whether managed objects associated with an operation are in the allowable range of a view. Only managed objects in the range of a view can be accessed.

Configuring an Authentication Name and Access Permission

Command	**snmp-server community** [*0* | *7*] *string* [**view** *view-name*] [[**ro** | **rw**] [**host** *ipaddr*]] [**ipv6** *ipv6-aclname* |*aclnum* | *aclname*]
Parameter Description	*0*: Indicates that the input community string is a plaintext string. *7*: Indicates that the input community string is a ciphertext string. *string*: Community string, which is equivalent to the communication password between the NMS and the SNMP agent. *view-name*: Specifies a view name for view-based management. **ro:** Indicates that the NMS can only read variables of the MIB. **rw:** The NMS can read and write variables of the MIB. *aclnum*: ACL number. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *aclname*: ACL name. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *ipaddr*: Associates NMS addresses and specifies NMS addresses for accessing the MIB. *ipv6-aclname*: IPv6 access list name, which specifies the IPv6 addresses that are permitted to access the MIB.
Command Mode	Global configuration mode
Usage Guide	This command is the first important command for enabling the SNMP agent function. It specifies community attributes and NMS scope where access to the MIB is allowed. To disable the SNMP agent function, run the **no snmp-server** command.

Configuring an SNMP User

Command	**snmp-server user** *username groupname* { **v1** | **v2c** | **v3** [**encrypted**] [**auth** { **md5** | **sha** } *auth-password*] [**priv des56** *priv-password*] } [**access** { **ipv6** *ipv6-aclname* | *aclnum* | *aclname* }]
Parameter Description	*username*: User name. *groupname*: Specifies the group name for a user. **v1** | **v2c** | **v3:** Specifies the SNMP version. Only SNMPv3 supports later security parameters. **encrypted:** The specified password input mode is ciphertext input. Otherwise, plaintext is used for input. If ciphertext input is selected, enter a key consisting of continuous hexadecimal digits. An MD5 protocol authentication key consists of 16 bytes and an SHA authentication protocol key consists of 20 bytes. Two characters stand for one byte. Encrypted keys are valid for this engine only. **auth:** Specifies whether authentication is used. **md5:** Specifies the MD5 authentication protocol. **sha** specifies the SHA authentication protocol. *auth-password*: Configures a password string (not more than 32 characters) used by the authentication protocol. The system converts the passwords into the corresponding authentication keys. **priv:** Specifies whether confidentiality is used. **des56** specifies the use of the 56-bit DES encryption protocol. *priv-password*: Configures a password string (not more than 32 characters) used for encryption. The system converts the password into the corresponding encryption key. *aclnum*: ACL number. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *aclname*: ACL name. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *ipv6-aclname*: IPv6 access list name, which specifies the IPv6 addresses that are permitted to access the MIB.
Command Mode	Global configuration mode
Usage Guide	Configure user information so that the NMS can communicate with the agent by using a valid user. For an SNMPv3 user, you can specify the security level, authentication algorithm (MD5 or SHA), authentication password, encryption algorithm (at present, only DES is available), and encryption password.

Enabling the Agent Function

Command	**enable service snmp-agent**
Parameter Description	
Configuration mode	Privileged mode.
Usage Guide	This command is used to enable the SNMP agent function of a device.

Enabling the SNMP Attack Protection and Detection Function

Command	**snmp-server authentication attempt** *times* **exceed** { **lock** | **lock-time** *minutes* | **unlock** }
Parameter Description	*times*: Number of continuous failed attempts. **lock:** After continuous authentication fails, the source IP address is permanently forbidden to initiate authentication for access. The administrator needs to manually unlock the IP address. **lock-time** *minutes*: After continuous authentication fails, the source IP address is forbidden to initiate authentication

	for access in a period of time. Beyond the period, the source IP address can be authenticated for access again. **unlock:** After continuous authentication fails, the source IP address is allowed to access the MIB continuously, which is equivalent to the fact that the SNMP attack protection and detection function is not configured.
Command Mode	Global configuration mode
Usage Guide	Configure the SNMP attack protection and detection function so that the corresponding measure can be taken after continuous authentication fails. The permanently forbidden source IP addresses can be authenticated for access again only after the administrator manually unlocks the IP addresses. The source IP address that are forbidden to access the MIB in a period of time can be authenticated for access again after the period expires or after the administrator manually unlocks the IP addresses.

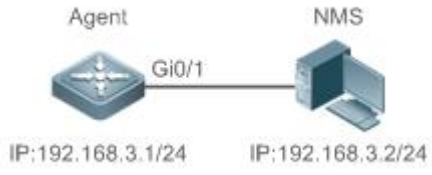
Setting Password Dictionary Check for Communities and Users

Command	**snmp-server enable secret-dictionary-check**
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	This command must be used with the **password policy** command to set check rules, for example, the password must consist of not less than six characters. To disable password dictionary check, run the **no snmp-server enable secret-dictionary-check** command.

Displaying the SNMP Status Information

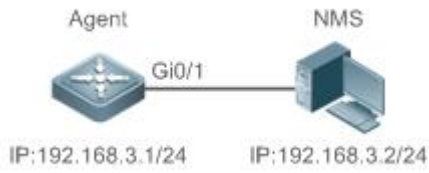
Command	**show snmp** [**mib** | **user** | **view** | **group**| **host** | **locked-ip** | **process-mib-time**]
Parameter Description	**mib:** Displays information about the SNMP MIB supported in the system. **user:** Displays information about an SNMP user. **view:** Displays information about an SNMP view. **group:** Displays information about an SNMP user group. **host:** Displays information about user configuration. **locked-ip:** Source IP address that is locked after continuous authentication fails. **process-mib-time:** Displays the MIB node with the longest processing time.
Configuration mode	Privileged mode.
Usage Guide	N/A

Configuration Example Configuring SNMP v1/2c

Scenario **Figure 4-5**	

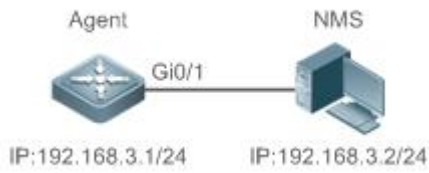
	● The NMS is connected to an agent through the Ethernet. The IP address of the agent is 192.168.3.1/24, and the IP address of the NMS is 192.168.3.2/24. ● The NMS monitors and manages the agent through SNMP v1 or SNMP v2c.
	● When the agent is faulty or an error occurs, the agent can actively report the related information to the NMS.
Configuration Steps	● Configure the SNMP basic information, including the version and community name. ● Allow the NMS (192.168.3.2/24) to send Trap messages. ● Configure the IP address of the agent, and set the IP address of the Gi0/1 interface to 192.168.3.1/24.
Agent	FS(config)#snmp-server community public rw FS(config)#snmp-server host 192.168.3.2 traps version 2c public FS(config)#snmp-server enable traps FS(config)#interface gigabitEthernet 0/1 FS(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0 FS(config-if-gigabitEthernet 0/1)#exit
Verification	● Run the **show running-config** command to display configuration information of the device. ● Run the **show snmp host** command to display the host information configured by the user.
NMS	On the NMS that uses the SNMP v1/v2c, configure the read/write community name, timeout time, and retry times. You can use the NMS to query and configure the device. ⚠ Configurations on the NMS must be consistent with those on the device; otherwise, related operations cannot be performed.

Configuring SNMP v3 (Default View)

Scenario **Figure 4-6**	 ● The NMS manages network devices (agents) based on the user authentication and encryption mode, for example, the NMS uses user1 as the user name, MD5 as the authentication mode, 123 as the authentication password, DES56 as the encryption algorithm, and 321 as the encryption password. ● You can access all MIB nodes. ("read default write default" indicates that all MIB nodes can be accessed.) ● Network devices can actively send authentication and encryption messages to the NMS.
Configuration Steps	● Configure an MIB group. Create a group “g1”, select the version “v3”, set the security level to the authentication and encryption mode “priv”, and configure permissions to read and write the view “default”. "Default" indicates that all MIB nodes can be accessed. ● Configure an SNMP user. Create a user named “user1” under group “g1”, select “v3” as the version, and set the authentication mode to “md5”, authentication password to “123”, encryption mode to “DES56”, and encryption password to “321”. ● Configure the SNMP host address. Set the host address to 192.168.3.2, select “3” as the version, set the security

	level to the authentication and encryption mode “priv”, and associate the user name “user1”. Enable the agent to actively send a trap message to the NMS. ● Configure the IP address of the agent. Set the address of the Gi0/1 interface to 192.168.3.1/24.
Agent	FS(config)#snmp-server group g1 v3 priv read default write default FS(config)#snmp-server user user1 g1 v3 auth md5 123 priv des56 321 FS(config)#snmp-server host 192.168.3.2 traps version 3 priv user1 FS(config)#snmp-server enable traps FS(config)#interface gigabitEthernet 0/1 FS(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0 FS(config-if-gigabitEthernet 0/1)#exit
Verification	● Run the **show running-config** command to display configuration information of the device. ● Run the **show snmp user** command to display the SNMP user. ● Run the **show snmp view** command to display the SNMP view. ● Run the **show snmp group** command to display the SNMP group. ● Run the **show snmp host** command to display the host information configured by the user. ● Install MIB-Browser.
NMS	SNMP v3 adopts the authentication and encryption security mechanisms. On the NMS, configure the user name, and select a security level. Based on the selected security level, configure the authentication mode, authentication password, encryption mode, and encryption password. In addition, configure the timeout time and retry times. You can use the NMS to query and configure the device. For details about the configuration, see Figure 2-7. ⚠ Configurations on the NMS must be consistent with those on the device; otherwise, related operations cannot be performed.

Configuring SNMPv3 Configuration (Specified View)

Scenario **Figure 4-7**	 ● The NMS manages network devices (agents) based on the user authentication and encryption mode, for example, the NMS uses user1 as the user name, MD5 as the authentication mode, 123 as the authentication password, DES56 as the encryption algorithm, and 321 as the encryption password. ● Network devices can control the operation permission of users to access MIB objects. For example, the user named user1 can read MIB objects under the system node (1.3.6.1.2.1.1) and can only write MIB objects under the SysContact node (1.3.6.1.2.1.1.4.0). ● Network devices can actively send authentication and encryption messages to the NMS.
Configuration	● Configure a MIB view and a MIB group. Create a MIB view “view1”, which includes the associated MIB object

Steps	(1.3.6.1.2.1.1); then create a MIB view "view2", which includes the associated MIB object (1.3.6.1.2.1.1.4.0). Create a group "g1", select the version "v3", set the security level to the authentication and encryption mode "priv", and configure permissions to read the view "view1" and write the view "view2". ● Configure an SNMP user. Create a user named "user1" under group "g1", select "v3" as the version, and set the authentication mode to "md5", authentication password to "123", encryption mode to "DES56", and encryption password to "321". ● Configure the SNMP host address. Set the host address to 192.168.3.2, select "3" as the version, set the security level to the authentication and encryption mode "priv", and associate the user name "user1". Enable the agent to actively send a trap message to the NMS. ● Set the IP address of the agent. Set the address of the Gi0/1 interface to 192.168.3.1/24.
Agent	FS(config)#snmp-server view view1 1.3.6.1.2.1.1 include FS(config)#snmp-server view view2 1.3.6.1.2.1.1.4.0 include FS(config)#snmp-server group g1 v3 priv read view1 write view2 FS(config)#snmp-server user user1 g1 v3 auth md5 123 priv des56 321 FS(config)#snmp-server host 192.168.3.2 traps version 3 priv user1 FS(config)#snmp-server enable traps FS(config)#interface gigabitEthernet 0/1 FS(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0 FS(config-if-gigabitEthernet 0/1)#exit
Verification	1. Run the **show running-config** command to display configuration information of the device. 2. Run the **show snmp user** command to display the SNMP user. 3. Run the **show snmp view** command to display the SNMP view. 4. Run the **show snmp group** command to display the SNMP group. 5. Run the **show snmp host** command to display the host information configured by the user. 6. Install MIB-Browser.

Agent	FS# show running-config
	!
	interface gigabitEthernet 0/1
	  no ip proxy-arp
	  ip address 192.168.3.1 255.255.255.0
	!
	snmp-server view view1 1.3.6.1.2.1.1 include
	snmp-server view view2 1.3.6.1.2.1.1.4.0 include
	snmp-server user user1 g1 v3 encrypted auth md5 7EBD6A1287D3548E4E52CF8349CBC93D priv des56 D5CEC4884360373ABBF30AB170E42D03
	snmp-server group g1 v3 priv read view1 write view2
	snmp-server host 192.168.3.2 traps version 3 priv user1
	snmp-server enable traps

	FS# show snmp user User name: user1 Engine ID: 800013110300d0f8221120 storage-type: permanent active

	Security level: auth priv Auth protocol: MD5 Priv protocol: DES Group-name: g1
	FS#show snmp view view1(include) 1.3.6.1.2.1.1 view2(include) 1.3.6.1.2.1.1.4.0 default(include) 1.3.6.1
	FS# show snmp group groupname: g1 securityModel: v3 securityLevel:authPriv readview: view1 writeview: view2 notifyview:
	FS#show snmp host Notification host: 192.168.3.2 udp-port: 162 type: trap user: user1 security model: v3 authPriv
	Install MIB-Browser, enter IP address 1**92.168.3.1** in **IP Address** and **user1** in **UserName**, select **AuthPriv** for **Security Level**, enter **123** in **AuthPassWord**, select **MD5** for **AuthProtocol**, and enter **321** in **PrivPassWord**. Click **Add Item** and select a management unit for which the MIB needs to be queried, for example, **System** in the following figure. Click **Start**. The MIB is queried for network devices. The lowest pane in the following figure shows query results.

Common Errors

4.4.2 Enabling the Trap Function

Configuration Effect

Enable the agent to actively send a trap message to the NMS.

Notes

N/A

Configuration Steps

Configuring the SNMP Host Address

- Optional
- Configure the host address of the NMS when the agent is required to actively send messages.

Enabling the Agent to Actively Send a Trap Message to the NMS

- Optional
- Configure this item on the agent when the agent is required to actively send a trap message to the NMS.

Enabling the Function of Sending a Link Trap Message on an Interface

- Optional
- Configure this item on the agent when a link trap message needs to be sent on an interface.

Enabling the Function of Sending a System Reboot Trap Message

- Optional
- Configure this item on the agent when the FSOS system is required to send a trap message to the NMS to notify system reboot before reloading or reboot of the device.

Specifying the Source Address for Sending a Trap Message

- Optional
- Configure this item on the agent when it is required to permanently use a local IP address as the source SNMP address to facilitate management.

Enabling a Trap Message to Carry Private Fields when the Message Is Sent

- Optional
- Configure this item on the agent when private fields need to be carried in a trap message.

Verification

Run the **show snmp** command to display the SNMP status.

Run the **show running-config** command to display configuration information of the device.

Related Commands

Setting the NMS Host Address

Command	**snmp-server host** [**oob**] { *host-addr* | **ipv6** *ipv6-addr* } [**traps** | **informs**] [**version** { **1** | **2c** | **3** { **auth** | **noauth** | **priv** }] *community-string* [**udp-port** *port-num*] [*notification-type*]
Parameter Description	**oob:** Configures Out-Of-Band (OOB) communication for the alarm server (that is, information is sent to the alarm server through the MGMT interface). *host-addr*: Address of the SNMP host. *ipv6-addr*: IPv6 address of the SNMP host. **traps | informs:** Configures the host to send a trap message or an inform message. **version:** SNMP version, which can be set to **V1**, **V2C**, or **V3**. **auth** | **noauth** | **priv:** Sets the security level of V3 users. *community-string*: Community string or user name (V3). *port-num*: Configures the port ID of the SNMP host. *notification-type*: Type of trap messages that are actively sent, for example, snmp. If no trap type is specified, all trap messages are sent.

Command Mode	Global configuration mode
Usage Guide	This command is used with the **snmp-server enable traps** command to actively send trap messages to the NMS. You can configure different SNMP hosts to receive trap messages. A host can support different traps and ports.

Enabling the Agent to Actively Send a Trap Message to the NMS

Command	**snmp-server enable traps** [*notification-type*]
Parameter Description	*notification-type*: Enables trap notification for the corresponding events, including the following types: snmp: Enables trap notification for SNMP events. bridge: Enables trap notification for bridge events. mac-notification: Enables trap notification for MAC events. ospf: Enables trap notification for OSPF events. vrrp: Enables trap notification for VRRP events. web-auth: Enables trap notification for Web authentication events.
Command Mode	Global configuration mode
Usage Guide	This command must be used with the **snmp-server host** command to so that trap messages can be actively sent.

Enabling the Function of Sending a Link Trap Message on an Interface

Command	**snmp trap link-status**
Parameter Description	-
Configuration mode	Interface configuration mode
Usage Guide	For interfaces (Ethernet interface, AP interface, and SVI interface), when this function is enabled, the SNMP sends a Link Trap message if the link status on the interfaces changes. Otherwise, the SNMP does not send the message.

Enabling the Function of Sending a System Reboot Trap Message

Command	**snmp-server system-shutdown**
Parameter Description	-
Configuration mode	Global configuration mode
Usage Guide	When the function of notification upon SNMP system reboot is enabled, a trap message is sent to the NMS to notify system reboot before reloading or reboot of the device.

Specifying the Source Address for Sending a Trap Message

Command	**snmp-server trap-source** *interface*
Parameter Description	*interface*: Used as the interface for the SNMP source address.

Configuration mode	Global configuration mode
Usage Guide	By default, the IP address of the interface where SNMP packets are sent is used as the source address. To facilitate management and identification, this command can be run to permanently use one local IP address as the source SNMP address.

Enabling a Trap message to Carry Private Fields when the Message Is Sent

Command	**snmp-server trap-format private**
Parameter Description	N/A
Configuration mode	Global configuration mode
Usage Guide	This command can be used to enable a trap message to carry private fields when the message is sent. At present, supported private fields include the alarm generation time. For the specific data types and data ranges of the fields, see FS-TRAP-FORMAT-MIB.mib.

Configuration Example

Enabling the Trap Function

Scenario Figure 4-8	 ● The NMS manages network devices (agents) based on the community authentication mode, and network devices can actively send messages to the NMS.
Configuration Steps	1. Perform configuration to enable the agent to actively send messages to the NMS. Set the SNMP host address to 192.168.3.2, the message format to Version2c, and the authentication name to user1. Enable the agent to actively send trap messages. 2. Set the IP address of the agent. Set the address of the Gi0/1 interface to 192.168.3.1/24.
Agent	FS(config)#snmp-server host 192.168.3.2 traps version 2c user1 FS(config)#snmp-server enable traps FS(config)#interface gigabitEthernet 0/1 FS(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0 FS(config-if-gigabitEthernet 0/1)#exit
Verification	● Run the **show running-config** command to display configuration information of the device. ● Run the **show snmp** command to display the SNMP status.
Agent	FS# show running-config ip access-list standard a1 10 permit host 192.168.3.2

	interface gigabitEthernet 0/1
	  no ip proxy-arp
	  ip address 192.168.3.1 255.255.255.0
	snmp-server view v1 1.3.6.1.2.1.1 include
	snmp-server location fuzhou
	snmp-server host 192.168.3.2 traps version 2c user1
	snmp-server enable traps
	snmp-server contact FS.com.cn
	snmp-server community user1 view v1 rw a1
	snmp-server chassis-id 1234567890

	FS#show snmp
	Chassis: 1234567890
	0 SNMP packets input
	  0 Bad SNMP version errors
	  0 Unknown community name
	  0 Illegal operation for community name supplied
	  0 Encoding errors
	  0 Number of requested variables
	  0 Number of altered variables
	  0 Get-request PDUs
	  0 Get-next PDUs
	  0 Set-request PDUs
	0 SNMP packets output
	  0 Too big errors (Maximum packet size 1472)
	  0 No such name errors
	  0 Bad values errors
	  0 General errors
	  0 Response PDUs
	  0 Trap PDUs
	SNMP global trap: enabled
	SNMP logging: disabled
	SNMP agent: enabled

Common Errors

N/A

4.4.3 Shielding the Agent Function

Configuration Effect

Shield the agent function when the agent service is not required.

Notes

- Run the **no snmp-server** command to shield the SNMP agent function when the agent service is not required.

- Different from the shielding command, after the **no enable service snmp-agent** command is run, all SNMP services are directly disabled (that is, the SNMP agent function is disabled, no packet is received, and no response packet or trap packet is sent), but configuration information of the agent is not shielded.

Configuration Steps

Shielding the SNMP Agent Function for the Device

- Optional
- To shield the configuration of all SNMP agent services, use this configuration.

Disabling the SNMP Agent Function for the Device

- Optional
- To directly disable all services, use this configuration.

Verification

Run the **show services** command to check whether SNMP services are enabled or disabled.

Run the **show snmp** command to display the SNMP status.

Run the **show running-config** command to display configuration information of the device.

Related Commands

Shielding the SNMP Agent Function for the Device

Command	**no snmp-server**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, the SNMP agent function is disabled. When SNMP agent parameters (for example, NMS host address, authentication name, and access permission) are set, the SNMP agent service is automatically enabled. The **enable service snmp-agent** command must also be run at the same time so that the SNMP agent service can take effect. If the SNMP agent service is disabled or the **enable service snmp-agent** command is not run, the SNMP agent service does not take effect. Run the **no snmp-server** command to disable SNMP agent services of all versions supported by the device. After this command is run, all SNMP agent service configurations are shielded (that is, after the **show running-config** command is run, no configuration is displayed. Configurations are restored after the SNMP agent service is enabled again). After the **enable service snmp-agent** command is run, the SNMP agent configurations are not shielded.

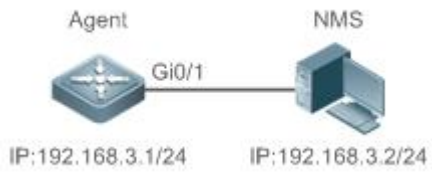
Disabling the SNMP Agent Function for the Device

Command	**no enable service snmp-agent**
Parameter Description	N/A
Configuration	Global configuration mode

mode	
Usage Guide	disable the SNMP service, but it will not shield SNMP agent parameters.

Configuration Example

Enabling the SNMP Service

Scenario **Figure 4-9**	 After the SNMP service is enabled and the SNMP agent server is set, the NMS can access devices based on SNMP.
Configuration Steps	1. Enable the SNMP service. 2. Set parameters for the SNMP agent server to make the SNMP service take effect.
A gent	FS(config)#enable service snmp-agent
Verification	1. Run the **show services** command to check whether the SNMP service is enabled or disabled.
Agent	FS#show service web-server : disabled web-server(https): disabled snmp-agent : enabled ssh-server : disabled telnet-server : enabled

Common Errors

N/A

4.4.4 Setting SNMP Control Parameters

Configuration Effect

Set basic parameters of the SNMP agent, including the device contact mode, device location, serial number, and parameters for sending a trap message. By accessing the parameters, the NMS can obtain the contact person of the device and physical location of the device.

Notes

N/A

Configuration Steps

Setting the System Contact Mode

- Optional
- When the contact mode of the system needs to be modified, configure this item on the agent.

Setting the System Location

- Optional
- When the system location needs to be modified, configure this item on the agent.

Setting the System Serial Number

- Optional
- When the system serial number needs to be modified, configure this item on the agent.

Setting NE Information about the Device

- Optional
- When the NE code needs to be modified, configure this item on the agent.

Setting the Maximum Packet Length of the SNMP Agent

- Optional
- When the maximum packet length of the SNMP agent needs to be modified, configure this item on the agent.

Setting the UDP Port ID of the SNMP Service

- Optional
- When the UDP port ID of the SNMP service needs to be modified, configure this item on the agent.

Setting the Queue Length of Trap Messages

- Optional
- When the size of the message queue needs to be adjusted to control the message sending speed, configure this item on the agent.

Setting the Interval for Sending a Trap Message

- Optional
- When the interval for sending a trap message needs to be modified, configure this item on the agent.

Configuring SNMP Flow Control

- Optional
- If a large number of SNMP request packets result in high CPU usage for SNMP tasks, configure SNMP flow control to limit the number of request packets processed per second in each SNMP task, so as to control the CPU usage for SNMP tasks.

Verification

Run the **show snmp** command to display the SNMP status.

Run the **show running-config** command to display configuration information of the device.

Related Commands

Setting the System Contact Mode

Command	**snmp-server contact** *text*

Parameter Description	*text*: String that describes the system contact mode.
Command Mode	Global configuration mode
Usage Guide	N/A

Setting the System Location

Command	**snmp-server location** *text*
Parameter Description	*text*: String that describes system information.
Configuration mode	Global configuration mode
Usage Guide	N/A

Setting the System Serial Number

Command	**snmp-server chassis-id** *text*
Parameter Description	*text*: Text of the system serial number, which may be digits or characters.
Configuration mode	Global configuration mode
Usage Guide	In general, the device serial number is used as the SNMP serial number to facilitate identification of the device.

Setting NE Information about the Device

Command	**snmp-server net-id** *text*
Parameter Description	*text*: Text that is used to set the device NE code. The text is a string that consists of 1 to 255 characters that are case-sensitive and may include spaces.
Configuration mode	Global mode.
Usage Guide	Set the NE code of the device.

Setting the Maximum Packet Length of the SNMP Agent

Command	**snmp-server packetsize** *byte-count*
Parameter Description	*byte-count*: Packet size, ranging from 484 bytes to 17,876 bytes.
Configuration mode	Global mode.
Usage Guide	N/A

Setting the UDP Port ID of the SNMP Service

Command	**snmp-server udp-port** *port-num*

Parameter Description	*port-num*: Specifies the UDP port ID of the SNMP service, that is, the ID of the protocol port that receives SNMP packets.
Configuration mode	Global mode.
Usage Guide	Specify the protocol port ID for receiving SNMP packets.

Setting the Length of a Trap Message Queue

Command	**snmp-server queue-length** *length*
Parameter Description	*length*: Queue length, ranging from 1 to 1,000.
Configuration mode	Global configuration mode
Usage Guide	Adjust the size of the message queue to control the message sending speed.

Setting the Interval for Sending a Trap Message

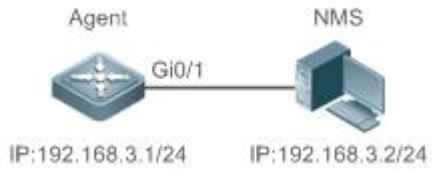
Command	**snmp-server trap-timeout** *seconds*
Parameter Description	*seconds*: Interval (unit: second). The value range is 1 to 1,000.
Configuration mode	Global configuration mode
Usage Guide	Adjust the interval for sending a message to control the message sending speed.

Configuring SNMP Flow Control

Command	**snmp-server flow-control pps** [*count*]
Parameter Description	*count*: Number of SNMP request packets processed per second. The value range is 50 to 65,535.
Command Mode	Global configuration mode
Usage Guide	If a large number of SNMP request packets result in high CPU usage for SNMP tasks, configure SNMP flow control to limit the number of request packets processed per second in each SNMP task, so as to control the CPU usage for SNMP tasks.

Configuration Example

Setting SNMP Control Parameters

Scenario **Figure 4-10**	

	● The NMS manages network devices (agents) based on the community authentication mode and can obtain basic system information about the devices, for example, system contact mode, location, and serial number.
Configuration Steps	1. Set SNMP agent parameters. Set the system location, contact mode, and serial number. 2. Set the IP address of the agent. Set the address of the Gi0/1 interface to 192.168.3.1/24.
Agent	FS(config)#snmp-server location fuzhou FS(config)#snmp-server contact FS.com.cn FS(config)#snmp-server chassis-id 1234567890 FS(config)#interface gigabitEthernet 0/1 FS(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0 FS(config-if-gigabitEthernet 0/1)#exit
Verification	1. Check the configuration information of the device. 2. Check the SNMP view and group information.

Agent	FS# show running-config
	ip access-list standard a1
	  10 permit host 192.168.3.2
	interface gigabitEthernet 0/1
	  no ip proxy-arp
	  ip address 192.168.3.1 255.255.255.0
	snmp-server view v1 1.3.6.1.2.1.1 include
	snmp-server location fuzhou
	snmp-server host 192.168.3.2 traps version 2c user1
	snmp-server enable traps
	snmp-server contact FS.com.cn
	snmp-server community user1 view v1 rw a1
	snmp-server chassis-id 1234567890

	FS#show snmp view v1(include) 1.3.6.1.2.1.1 default(include) 1.3.6.1 FS#show snmp group groupname: user1 securityModel: v1 securityLevel:noAuthNoPriv readview: v1 writeview: v1 notifyview: groupname: user1 securityModel: v2c securityLevel:noAuthNoPriv readview: v1 writeview: v1 notifyview:

Common Errors

N/A

4.5 Monitoring

Clearing

Description	Command
Clears the list of source IP addresses that are locked after continuous authentication fails.	**clear snmp locked-ip** [**ipv4** *ipv4-address* | **ipv6** *ipv6-address*]

Displaying

Description	Command
Displays the SNMP status.	**show snmp** [**mib** | **user** | **view** | **group**| **host**]

5 Configuring CM-APM

5.1 Overview

The centralized management (CM) and application performance management (APM) are the centralized management and performance monitoring functions provided by FS gateways. The functions must be used in combination with the remote auto-management center (RAC) software.

The functions can implement centralized management of gateways and monitor gateway performance, VPN, traffic, and services globally, which significantly improves the working efficiency of the NMS.

FS CM-APM is generally applied to headquarters/branch enterprises, chain hotels, and metropolitan area networks (MANs) of general education for managing multiple gateways at the same time.

5.2 Applications

Application	Description
Centralized Management and Performance Monitoring of Network-wide Gateways for Headquarters/Branch Enterprises	In the typical network topology of a headquarter/branch enterprise, office software servers (such as Web and ERP software) and data centers are deployed in the enterprise headquarters. Gateways (such as EGs) are deployed on the egress interfaces of the enterprise headquarters and branches.

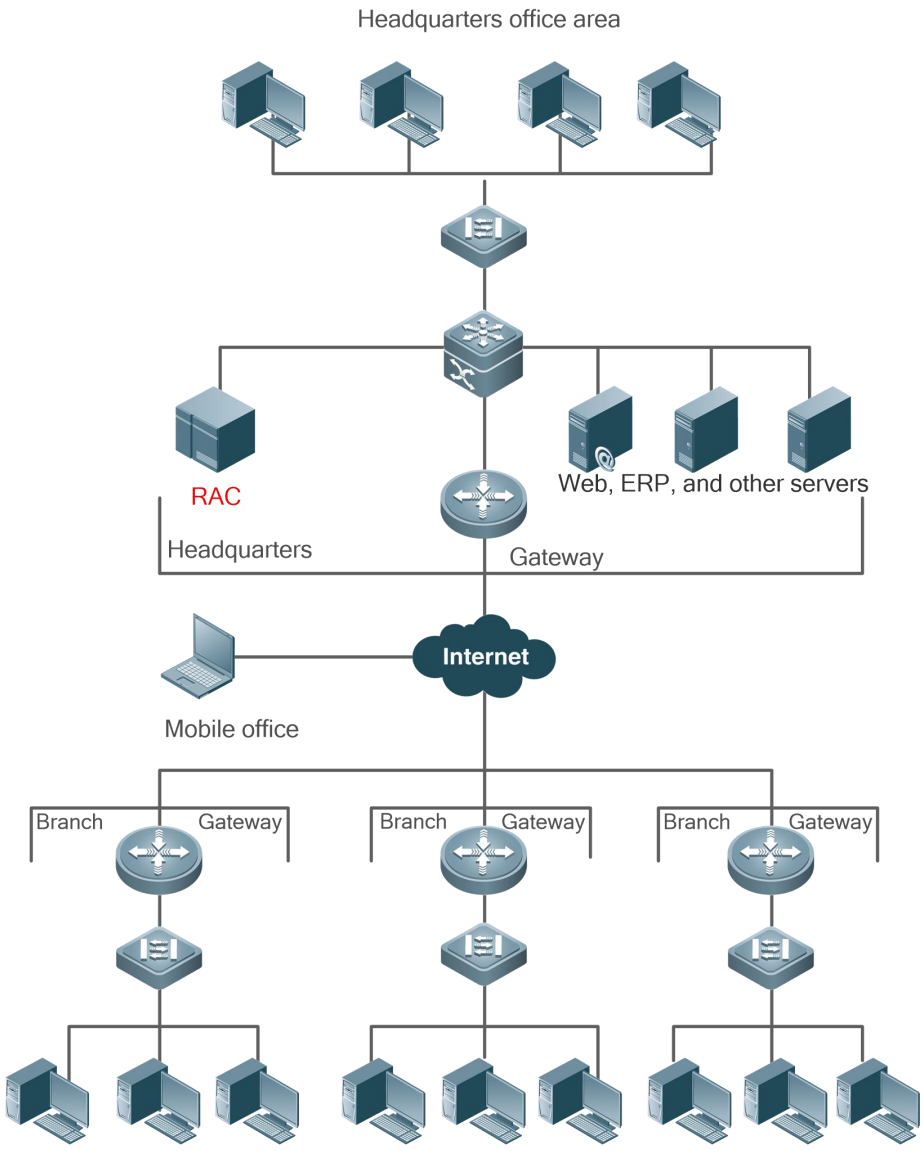
5.2.1 Centralized Management and Performance Monitoring of Network-wide Gateways for Headquarters/Branch Enterprises

Scenario

In the typical network topology of a headquarter/branch enterprise, office software servers (such as Web and ERP software) and data centers are deployed in the enterprise headquarters. Gateways (such as EGs) are deployed on the egress interfaces of the enterprise headquarters and branches. Generally, the headquarters (fiber line connection) is provided with a high bandwidth and multiple lines; branches (ADSL connection) are provided with a low bandwidth. The Web and ERP systems in the headquarters are operated and maintained by the information and resource department, which is responsible for business server maintenance. Access to the Web and ERP systems falls into the following scenarios:

- A user in the headquarters directly accesses the business system. Since the access is implemented on the intranet, user experience is good provided that the business server is normal.
- A user in a branch accesses the business system. In this case, user experience may be affected by network limitations.
- A mobile user accesses the business system from an extranet via a VPN. In this case, user experience may be affected by network limitations as well.

Figure 5-1



Remarks	The gateways are egress gateways. The RAC is FS NMS software.

Deployment

- Enable the application identification, L2/L3 identification, and flow audit functions on the gateways throughout the network.
- Enable gateway status (CPU, memory, and hard disk) monitoring throughout the network.
- Enable VPN status monitoring of branch gateways.
- Enable traffic and bandwidth monitoring of branch gateways.
- Monitor the loading time consumed by branches to access headquarters intranet.

5.3 Features

Basic Concepts

Delay

Delay indicates the time required for transmitting a packet across a network.

HTTP GET

The hypertext transport protocol (HTTP) defines communication rules used between a browser and web server and transmits files over the Internet. The HTTP GET is a type of HTTP request. Generally, web browsing is implemented by HTTP GET requests.

Overview

Feature	Description
Gateway Status Monitoring	The RAC monitors use of the CPU, memory, and hard disk of all gateways in a centralized manner, which helps discover problems in a timely manner.
VPN Status Monitoring	In the headquarters/branch enterprise scenario, branches implement virtual private-line connection with the headquarters over VPNs, so that branch access requests are carried over the VPN lines. The quality of VPN lines directly affects the office efficiency of the branches. The RAC monitors the VPN status of the branch gateways, which helps discover problems in a timely manner and minimize impact on the branch office.
Bandwidth Status Monitoring	The RAC monitors the bandwidth use of all gateways in a centralized manner, which helps discover problems in a timely manner.
Service Loading Throughput Monitoring	The RAC monitors and visualizes service loading throughputs of all gateways in a centralized manner, which helps discover service loading throughput problems in a timely manner.
Ping Test	Ping test is used to detect network abnormalities. The RAC monitors the ping test results of all gateways, which helps discover network abnormalities in a timely manner.
Behavior Report URL-TOPN	With CM-APM, users can learn the most frequently accessed URLs, analyze working efficiency according to user behaviors, and use the monitoring result as a basis for advertisement.
Webpage Loading Time Monitoring	Upon webpage loading throughput complaints, customers can use CM-APM to quantify the webpage loading throughputs, thereby determining whether the problem exists or merely reflecting the subjective feeling of partial users.
Video Conference Quality Monitoring	The RAC monitors the video conference quality of the entire network, which helps discover problems in a timely manner.

5.3.1 Gateway Status Monitoring

The RAC monitors use of the CPU, memory, and hard disk of all gateways in a centralized manner, which helps discover problems in a timely manner.

Working Principle

A gateway periodically collects the utilization rates of its CPU, memory, and hard disk, and sends the sample data to the RAC for centralized monitoring.

Related Configuration

Enabling Gateway Status Monitoring

The function is disabled by default.

Run the **apm sample enable** command to enable the function.

If the global monitoring function is enabled, run the **apm sample cpu-mem disable** and **apm sample sata-flash disable** commands to disable the function for a gateway.

Changing Monitoring Period

The gateway status monitoring period is five minutes by default.

Run the **apm sample default interval** *second* command to change the global monitoring period. The value ranges from 10 to 3600 seconds.

Run the **apm sample cpu-mem interval** *second* and **apm sample sata-flash interval** *second* commands to separately change the monitoring period of a gateway.

A shorter monitoring period indicates a more real-time RAC monitoring result. However, a too short monitoring period may cause the gateway and RAC server to be overloaded.

5.3.2 VPN Status Monitoring

In the headquarters/branch enterprise scenario, branches implement virtual private-line connection with the headquarters over VPNs, so that branch access requests are carried over the VPN lines. The quality of VPN lines directly affects the office efficiency of the branches. The RAC monitors the VPN status of the branch gateways, which helps discover problems in a timely manner and minimize impact on the branch office.

Working Principle

A gateway periodically collects the VPN and traffic information and sends the sample data to the RAC for centralized monitoring.

Related Configuration

Enabling VPN Status Monitoring

The function is disabled by default.

Run the **apm sample enable** command to enable the function.

If the global monitoring function is enabled, run the **apm sample vpn disable disable** and **apm sample vpn-detail disable** commands to separately disable the function for a gateway.

Changing Monitoring Period

The gateway status monitoring period is five minutes by default.

Run the **apm sample default interval** *second* command to change the global monitoring period. The value ranges from 10 to 3600 seconds.

Run the **apm sample vpn interval** *second* and **apm sample vpn-detail interval** *second* commands to separately change the monitoring period of a gateway.

A shorter monitoring period indicates a more real-time RAC monitoring result. However, a too short monitoring period may cause the gateway and RAC server to be overloaded.

5.3.3 Bandwidth Status Monitoring

The RAC monitors the bandwidth use of all gateways in a centralized manner, which helps discover problems in a timely manner.

Working Principle

A gateway periodically collects information about the gateway IP address/session quantity, interface traffic, application traffic, traffic of an application type, and user traffic from the flow audit module and sends the sample data to the RAC for centralized monitoring.

Related Configuration

Enabling Bandwidth Status Monitoring

The function is disabled by default.

Run the **apm sample enable** command to enable the function.

If the global monitoring function is enabled, run the **apm sample ip-session disable**, **apm sample intf-flowrate disable**, **apm sample app-type-flowrate disable**, **apm sample app-flowrate disable**, and **apm sample user-flowrate disable** commands to separately disable the function for a gateway.

Changing Monitoring Period

The gateway status monitoring period is five minutes by default.

Run the **apm sample default interval** *second* command to change the global monitoring period. The value ranges from 10 to 3600 seconds.

Run the **apm sample ip-session interval** *second*, **apm sample intf-flowrate interval** *second*, **apm sample app-type-flowrate interval** *second*, **apm sample app-flowrate interval** *second*, and **apm sample user-flowrate interval** *second* commands to separately change the monitoring period of a gateway.

A shorter monitoring period indicates a more real-time RAC monitoring result. However, a too short monitoring period may cause the gateway and RAC server to be overloaded.

5.3.4 Service Loading Throughput Monitoring

The RAC monitors and visualizes service loading throughputs of all gateways in a centralized manner, which helps discover service loading throughput problems in a timely manner.

Working Principle

A gateway periodically collects data loading throughputs of specific services and sends the sample data to the RAC for centralized monitoring.

Related Configuration

Enabling Service Loading Throughput Monitoring

The function is disabled by default.

Run the **apm sample enable** command to enable the function, and run the **apm sample business application** *app-name* command to add services (applications) to be monitored. The **app-name** parameter indicates an application name.

If the global monitoring function is enabled, run the **apm sample ip-session business disable** command to separately disable the function for a gateway, or run the **no apm sample business application all** command to delete all services that need to be monitored.

Changing Monitoring Period

The gateway status monitoring period is five minutes by default.

Run the **apm sample default interval** *second* command to change the global monitoring period. The value ranges from 10 to 3600 seconds.

Run the **apm sample business interval** *second* command to separately change the monitoring period of a gateway.

A shorter monitoring period indicates a more real-time RAC monitoring result. However, a too short monitoring period may cause the gateway and RAC server to be overloaded.

5.3.5 Ping Test

Ping test is used to detect network abnormalities. The RAC monitors the ping test results of all gateways, which helps discover network abnormalities in a timely manner.

Working Principle

A gateway periodically pings a specified server and sends the ping test results to the RAC for centralized monitoring.

Related Configuration

Enabling Ping Test

The function is disabled by default.

Run the **apm sample enable** command to enable the function, and run the **apm sample ping-detect serve** command to add server IP addresses to be pinged.

If the global monitoring function is enabled, run the **apm sample ping-detect disable** command to separately disable the function for a gateway, or run the **no apm sample ping-detect server all** command to delete all servers to be pinged.

Modifying Ping Test Parameters

The gateway status monitoring period is five minutes by default.

Run the **apm sample default interval** *second* command to change the global monitoring period. The value ranges from 10 to 3600 seconds.

Run the **apm sample ping-detect interval** *second* command to separately change the monitoring period of a gateway.

A shorter monitoring period indicates a more real-time RAC monitoring result. However, a too short monitoring period may cause the gateway and RAC server to be overloaded.

5.3.6 Behavior Report URL-TOPN

With CM-APM, users can learn the most frequently accessed URLs, analyze working efficiency according to user behaviors, and use the monitoring result as a basis for advertisement.

Working Principle

The behavior report URL-TOPN is supported by the URL audit function of a gateway. The gateway periodically collects statistical information about the most frequently accessed URLs and sends the statistical result to the RAC for centralized monitoring.

Related Configuration

Enabling URL-TOPN

The function is disabled by default.

Run the **apm sample enable** command to enable the function.

If the global monitoring function is enabled, run the **apm sample url-topn disable** command to separately disable the function for a gateway.

Modifying URL-TOPN Parameters

After the global monitoring function is enabled, the top 50 URLs are collected by default. Run the **apm sample url-topn top** *num* command to change the number of top URLs. The value ranges from 1 to 100.

By default, the URL-TOPN behavior report is collected at 01:00 each day and contains data about the previous day. Run the **apm sample url-topn send-time** *hour* command to change the collection time.

Generally, the collection time is set to the idle time of the gateway to avoid impact on normal service running of the gateway.

5.3.7 Webpage Loading Time Monitoring

Upon webpage loading throughput complaints, customers can use CM-APM to quantify the webpage loading throughputs, thereby determining whether the problem exists or merely reflecting the subjective feeling of partial users.

Working Principle

A gateway monitors HTTP GET requests in real time and records the procedure from HTTP GET requests to responses to obtain the webpage loading time, and then sends the data to the RAC for centralized monitoring.

Related Configuration

Enabling Webpage Loading Time Monitoring

The function is disabled by default.

Run the **apm webpage url** *string* command to add URLs to be monitored. The webpage loading time monitoring function is enabled.
Run the **no apm webpage url all** command to disable the function.
Run the **no apm webpage enable** command to disable the function without deleting URL entries.

5.3.8 Video Conference Quality Monitoring

The RAC monitors the video conference quality of the entire network, which helps discover problems in a timely manner.

Working Principle

A gateway monitors the data flows of video conferences in real time, measures the delay, packet loss rate, and disorder indicators, and calculates the quality of the video conferences according to the performance data. Finally, the gateway sends the calculation result to the RAC for centralized monitoring.

Related Configuration

Monitoring Video Conference Quality

The function is disabled by default.

Run the **apm conference-system** { **application** *app-name* } | { **access-list** *acl_id* **alias** *alias-name* } command to add the data flows to be monitored. The video conference quality monitoring function is enabled.

Run the **no apm conference-system application all** and **no apm conference-system access-list all** commands to disable the function.

Run the **no apm conference-system enable** command to disable the function without deleting applications or ACLs.

5.4 Configuration

Configuration	Description and Command	
Configuring APM Log Servers	(Mandatory) It is used to send APM information.	
	apm server	Sets an APM log server.
	apm log-type	Specifies log server to which APM logs will be sent.
	apm export-rate	Sets APM log transmission rate.
	apm export-length	Sets the maximum length of valid packet data.
	apm template send-period	Sets APM template transmission period.
Configuring APM Monitoring Information	(Mandatory) It is used to enable APM monitoring functions.	
	apm sample enable	Enables global APM monitoring.
	apm sample disable	Disables specified APM monitoring functions.
	apm sample interval	Sets APM monitoring period.
	apm sample ping-detect	Sets ping test parameters.
	apm sample url-topn	Sets URL-TOPN parameters.
	apm webpage	Configures webpage loading time monitoring.
	apm conference-system	Configures video conference quality monitoring.

5.4.1 Configuring APM Log Servers

Configuration Effect

- Configure the information about APM log servers, including IP addresses, ports, and protocols.
- Specify log servers to which APM logs will be sent.

Notes

- After the information about the APM log servers is configured, specify log servers to which logs of different types will be sent.

Configuration Steps

Setting APM Log Servers

- Mandatory.
- Set one default log server unless otherwise specified.

Specifying Log Server to Which APM Logs Will Be Sent

- Mandatory.
- Unless otherwise specified, specify a default log server to which all logs will be sent.

Setting APM Log Transmission Rate

- Optional.
- Use the default value unless otherwise specified. If the transmission rate is too high, gateway CPU usage may be excessively high when there is a great deal of APM log information.

Setting Maximum Length of Valid Packet Data

- Optional.
- Use the default value unless otherwise specified.

Setting APM Template Transmission Period

- Optional.
- Use the default value unless otherwise specified.

Verification

Enable the APM monitoring function and set the APM log server and corresponding log type.

- Check whether the RAC server receives corresponding packets.
- Run the show apm server log-count command to display the number of transmitted logs.

Related Commands

Setting APM Log Server

Command	**apm server** *name* { *ip-address* } [**source** *ip-address*] [*port*] [**tcp** | **udp**] [**oob**]
Parameter Description	*name*: Indicates the name of an APM log server. *ip-address*: Indicates the IP address of the APM log server. *port*: Indicates the port number of the APM log server.
Command Mode	Global configuration mode
Usage Guide	Specify the TCP or UDP protocol for APM log transmission. TCP is the default and recommended protocol. A source IP address is configured during socket creation to resolve VPN problems. If the APM log server does not have a source IP address originally and no source IP address is configured, the value of this parameter is 0. If the APM log server has a source IP address originally, this source IP address is used and other parameters are updated according to the configuration. If a source IP address is configured, this configured IP address is used. If logs are transmitted through a management interface, specify the keyword **oob**. To delete a server, run the **no apm server** *name* command.

Specifying Log Server to Which APM Logs Will Be Sent

Command	**apm log-type** { *type* | **default** } **priority** *prio* **server** *name*
Parameter	*type*: Indicates APM log type. Run the **show apm log-type** command to display the log type indicated by each value.

Description	*prio*: Indicates a priority of a log type. The value ranges from 0 to 2. The value 0 indicates the highest priority.
Command Mode	Global configuration mode
Usage Guide	Specify priorities of log types and the APM log server to which the logs will be sent. A log can be sent to one server only. The parameter **default** indicates all logs are sent to the default server, unless otherwise specified. Generally, one default server is configured. To delete all log types, run the **no apm log-type all** command. To delete all log types of the default server, run the **no apm log-type default** command. To delete a certain log type, run the **no apm log-type** *type* command. The log type has been specified in a server already.

Setting APM Log Transmission Rate

Command	**apm export-rate** *rate*
Parameter Description	*Rate*: Indicates the number of APM logs that are sent per second. The value ranges from 10 to 100,000.
Command Mode	Global configuration mode
Usage Guide	The default transmission rate is 1000 logs per second. The default value is used unless otherwise specified. A too high value may cause excessively high CPU usage, and a too low value may cause log information loss.

Setting Maximum Length of Valid Packet Data

Command	**apm export-length** *value*
Parameter Description	*Value*: Indicates the length of valid data in ipfix packets. The length is measured from the TCP or UDP valid data (unit: byte). The value ranges from 300 to 1400.
Command Mode	Global configuration mode
Usage Guide	The default value is 1400. Generally, this parameter does not need to be configured and the default value is used. If the parameter is set to a larger value, bandwidth consumption is reduced.

Setting APM Template Transmission Period

Command	**apm template send-period** *seconds*
Parameter Description	*Seconds*: Indicates the template transmission duration (unit: second). The value ranges from 60 to 3600.
Command Mode	Global configuration mode
Usage Guide	The default value is five minutes. The APM log server (namely, the RAC server) extracts and parses log formats according to the template and periodically sends the template to the server, thereby avoiding log parsing failure in the event of server template loss (caused by restart or during startup).

Configuration Example

For details, refer to section 1.4.2.

Common Errors

- No log type is specified for the APM log server. Consequently, the RAC server will not receive APM relevant information.

5.4.2 Configuring APM Monitoring Information

Configuration Effect

- Enable the global APM monitoring function. Gateways collect information such as CPU usage, memory usage, hard disk status, VPN status, bandwidth status, service loading throughput, ping test, and behavior report URL-TOPN, and send the information to the RAC server.
- Enable the webpage loading time monitoring function and configure URLs to be monitored. Gateways monitor the webpage loading time and send the information to the RAC server.
- Enable the video conference quality monitoring function and configure applications or ACLs to be monitored. Gateways assess quality of the video conferences and send the assessment result to the RAC server.

Notes

- The gateway status monitoring, VPU status monitoring, bandwidth status monitoring, service loading throughput monitoring, ping test, and behavior report URL-TOPN functions can be enabled only after the global monitoring function is enabled by running the **apm sample enable** command. After the global monitoring function is enabled, these functions can be separately disabled.
- Only gateways with hard disks support the behavior report URL-TOPN.

Configuration Steps

Enabling Global APM Monitoring

- Mandatory.
- To enable the gateway status monitoring, VPU status monitoring, bandwidth status monitoring, service loading throughput monitoring, ping test, and behavior report URL-TOPN functions, enable the global APM monitoring function first.

Disabling Specified APM Monitoring Functions

- Optional.
- After the global APM monitoring function is enabled, specific functions can be separately disabled.

Setting APM Monitoring Period

- Optional.
- Use the default value unless otherwise specified.
- A shorter the monitoring period indicates a more real-time RAC monitoring result. In this case, system resource consumption will increase.
- The behavior report URL-TOPN is transmitted once each day. The report transmission time is modifiable, but the collection period is not.

Setting Ping Test Parameters

- Mandatory.

- Specify the servers to be tested according to requirements.

Setting URL-TOPN Parameters

- Optional.
- Change URL-TOPN parameter configuration according to requirements. Use the default values unless otherwise specified.

Configuring Webpage Loading Time Monitoring

- Mandatory.
- Configure URLs to be monitored according to requirements. The URLs are the result of precise match. Generally, only the homepage loading time is monitored.

Configuring Video Conference Quality Monitoring

- Mandatory.
- Configure video conferences to be monitored according to requirements by specifying application names (supported by application identification) or ACLs (in the scenario where only the IP addresses of the video servers are known).

Verification

Enable the global APM monitoring function and configure the APM log server and log types.

- Check whether the RAC server receives corresponding packets.
- Run the **show apm server log-count** command to display the number of transmitted logs.

Related Commands

Enabling Global APM Monitoring

Command	**apm sample enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	To enable the gateway status monitoring, VPU status monitoring, bandwidth status monitoring, service loading throughput monitoring, ping test, and behavior report URL-TOPN functions, enable the global APM monitoring function first.

Setting Global APM Monitoring Period

Command	**apm sample default interval** *num*
Parameter Description	*num*: Indicates the default monitoring period (unit: second). The value ranges from 10 to 3600.
Command Mode	Global configuration mode
Usage Guide	The default monitoring period is five minutes unless otherwise specified. Run the **no apm sample default interval** command to restore the default value.

Setting Monitoring Periods of Different Monitoring Functions

Command	**apm sample** { **cpu-mem** | **sata-flash** | **vpn** | **vpn-detail** | **ip-session** | **intf-flowrate** | **app-type-flowrate** | **app-flowrate** | **user-flowrate** | **ping-detect** | **business** } **interval** *second*
Parameter Description	*second*: Indicates the monitoring period (unit: second). The value ranges from 10 to 3600.
Command Mode	Global configuration mode
Usage Guide	It is not necessary to set monitoring periods of different monitoring functions unless otherwise specified. Use the **no** form of this command to delete the special configuration and restore the global default configuration. cpu-mem: Indicates the CPU and memory usage. sata-flash: Indicates the hard disk and flash memory usage. vpn: Indicates VPN status (connected or disconnected). vpn-detail: Indicates the application traffic details of VPN lines. ip-session: Indicates the IP address and session quantity. intf-flowrate: Indicates the interface traffic. app-type-flowrate: Indicates the traffic of an application type. app-flowrate: Indicates the application traffic. user flowrate: Indicates the user traffic. ping-detect: Indicates a ping test. business: Indicates the business data loading throughput.

Disabling Specified APM Monitoring Functions

Command	**apm sample** { **cpu-mem** | **sata-flash** | **vpn** | **vpn-detail** | **ip-session** | **intf-flowrate** | **app-type-flowrate** | **app-flowrate** | **user-flowrate** | **ping-detect** | **business** } **disable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After the global APM monitoring function is enabled, run this command to disable specific APM monitoring functions. Use the **no** form of this command to enable the functions again (the global APM monitoring function must be enabled first). Run the **apm sample del-all-disable** command to enable all APM monitoring functions (the global APM monitoring function must be enabled first). For details about fields such as **cpu-mem**, refer to the preceding section.

Configuring Service (Application) to Be Monitored

Command	**apm sample business application** *app-name*
Parameter Description	*app-name* Indicates an application name. For details, refer to the document about APP-IDENTITY.
Command Mode	Global configuration mode
Usage Guide	Specify an application to enable data loading throughput monitoring, which relies on the accuracy of the application

	identification result. At present, a maximum of 50 applications can be specified.

Configuring Server to Be Pinged

Command	**apm sample ping-detect server** [*ip-address* / *host*] [**ntimes** *times*] [**length** *len*] [**source** { **lan** | *so-ip-address* | *interface-name* }]
Parameter Description	*ip-address*: Indicates the IP address to be pinged. *Host*: Indicates the domain name to be pinged. *times*: Indicates the number of packets for each ping test. The value ranges from 1 to 10. *len*: Indicates the length of a ping packet. The value ranges from 64 to 1400. *so-ip-address*: Indicates the source IP address in a ping packet. *interface-name*: Indicates an interface name.
Command Mode	Global configuration mode
Usage Guide	Generally, set only an IP address or domain name of a server to be pinged. For other parameters, use the default values. If the server to be pinged is accessed via the IPSec VPN, configure the **source lan** parameter to ensure that an IPSec tunnel is used. In other cases, this parameter can be not configured.

Setting Top URLs

Command	**apm sample url-topn top** *num*
Parameter Description	*num*: Specifies the number of top URLs to be collected. The value ranges from 1 to 100.
Command Mode	Global configuration mode
Usage Guide	Use this command to set the number of URLs to be collected and sent.

Setting URL-TOPN Transmission Time

Command	**apm sample url-topn send-time** *hour*
Parameter Description	*Hour*: Specifies the URL-TOPN transmission time. The value ranges from 0 to 23.
Command Mode	Global configuration mode
Usage Guide	The default transmission time is 01:00. Generally, set the transmission time to the idle time of gateways.

Configuring URLs to Be Monitored

Command	**apm webpage url** *string*
Parameter Description	string: Indicates the URLs to be monitored. The http:// is not included and the keyword **all** cannot be used. A maximum of 50 URLs can be configured, with each URL containing no more than 200 bytes.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure a URL to be monitored. Run the **no apm webpage url** *string* command to delete specified URLs, and run the **no apm webpage url all** command to delete all URLs.

Enabling Webpage Loading Time Monitoring

Command	**apm webpage enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Enable this function by default. Run the **no apm webpage enable** command to disable this function temporarily without deleting URLs being monitored.

Configuring Video Conferences to Be Monitored by Specifying Application

Command	**apm conference-system application** *app-name*
Parameter Description	app-name: Indicates an application name. This parameter cannot be set to **all**.
Command Mode	Global configuration mode
Usage Guide	Specify an application to configure video conferences to be monitored. To delete the configuration of an application, run the **no apm conference-system application** *app-name* command in global configuration mode. To delete the configuration of all applications, run the **no apm conference-system application all** command in global configuration mode.

Configuring Video Conferences to Be Monitored by Specifying ACL

Command	**apm conference-system access-list** *acl_id* **alias** *alias-name*
Parameter Description	*acl_id*: Indicates the ID of an ACL. The value ranges from 1 to 199. *alias-name:* Indicates the alias of data flows.
Command Mode	Global configuration mode
Usage Guide	Specify an ACL to configure video conferences to be monitored. To delete an ACL rule, run the **no apm conference-system access-list** *acl_id* command in global configuration mode. To delete all ACL rules, run the **no apm conference-system access-list all** command in global configuration mode.

Configuring Video Conference Monitoring Period

Command	**apm conference-system measure-period** *period-time*
Parameter Description	*period-time*: Indicates the monitoring period (unit: second). The value ranges from 30 to 120.
Command Mode	Global configuration mode
Usage Guide	The video conference monitoring period indicates the interval of quality monitoring assessment. The default value is 60 seconds. To restore the default configuration, run the **no apm conference-system measure-period** command in global configuration mode. Generally, this parameter does not need to be configured.

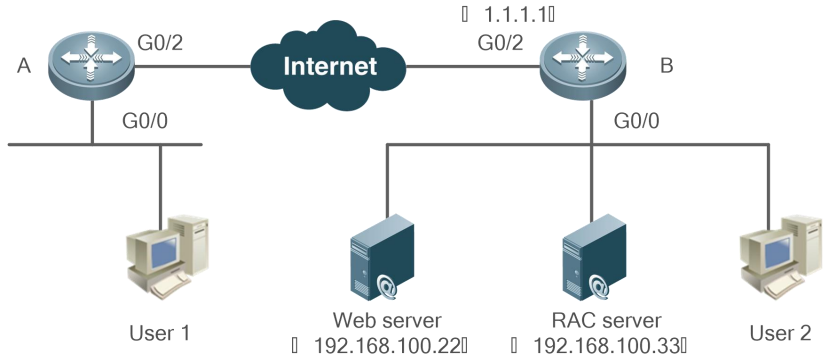
Enabling Video Conference Monitoring

Command	**apm conference-system enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Enable this function by default. Run the **no apm conference-system enable** command to disable this function temporarily without deleting applications and ACLs being monitored.

Configuration Example

Enabling Global APM Monitoring and Specifying Video Conference (InfowareLab Conference System) and URL (www.ietf.org) to Be Monitored and IP Address (192.168.100.22) of Server to Be Pinged (Branch Access Is Implemented over IPSec VPN)

Scenario Figure 5-2



Configuration Steps

- Map RAC relevant information on Gateway B to a public IP address.
- Set APM log server information on Gateway A and Gateway B.
- Specify a server to which all logs will be sent on Gateway A and Gateway B.
- Enable the global monitoring function on Gateway A and Gateway B.
- Enable the ping test function on Gateway A and Gateway B. Set the IP address to 192.168.100.22.
- Set the video conference to be monitored to InfowareLab conference system on Gateway A and Gateway B.
- Set the URL to be monitored to www.ietf.org on Gateway A and Gateway B.

A

```
A# configure terminal
A(config)# apm sample enable
A(config)# apm sample default interval 300
A(config)# apm sample ping-detect server 192.168.100.22 ntimes 5 length 100 source lan
A(config)# apm webpage url www.ietf.org/
A(config)# apm conference-system application InfowareLab conference system
A(config)# apm server rac 1.1.1.1 30000 tcp
A(config)# apm log-type default priority 1 server rac
```

B

```
B# configure terminal
B(config)# ip nat inside source static tcp 192.168.100.33 30000 interface gigabitEthernet 0/2 30000 permit-inside
B(config)# apm sample enable
B(config)# apm sample default interval 300
B(config)# apm sample ping-detect server 192.168.100.22 ntimes 5 length 100
B(config)# apm webpage url www.ietf.org/
B(config)# apm conference-system application InfowareLab conference system
```

	B(config)# apm server rac 192.168.100.33 30000 tcp B(config)# apm log-type default priority 1 server rac
Verification	● Verify that User 1 and User 2 hold a video conference using the InfowareLab conference system, and that the RAC server receives monitoring information from Gateway A and Gateway B. ● Verify that User 1 accesses www.ietf.org, and that the RAC server receives monitoring information from Gateway A. ● Verify that the RAC server periodically receives ping test information from Gateway A and Gateway B. ● Verify that the RAC server periodically receives other APM information from Gateway A and Gateway B.
A	A# show apm server log-count
B	B# show apm server log-count

Common Errors

- The name of the application with video conference enabled cannot be identified by a gateway, or the application name is set to **all**.
- A configured URL contains the header http://, resulting in identification error.
- A configured URL is not a specified webpage and does not end with /. For example, www.itef.org/ is changed to www.ietf.org.
- The server to be pinged is not accessed via IPSec VPN, but the **source lan** parameter is configured.

5.5 Monitoring

Clearing

Description	Command
Clears transmission statistics about APM logs.	**clear apm server log-count**

Displaying

Description	Command
Displays APM log server configuration.	**show apm server info**
Displays the number of transmitted APM logs.	**show apm server log-count**
Displays collection periods of different services.	**show apm sample log-sends**
Displays user-defined ping test or URL-TOPN information.	**show apm sample ping-detect info**
Displays user-defined URL-TOPN information.	**show apm sample url-topn info**
Displays services (applications) with the data loading throughput to be monitored.	**show apm sample business info**
Displays URLs to be monitored.	**show apm webpage url**

Displays webpage loading time monitoring result.	**show apm webpage statistics**
Displays UDP flow information of video conferences.	**show apm udp-measure info**
Displays TCP flow information of video conferences.	**show apm tcp-measure info**

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs the webpage loading time monitoring switch.	**debug apm webpage info**

6 Configuring ANTI-SNIPER

6.1 Overview

NetSniper can automatically detect the proxy server systems set up without authorization or unauthorized routers on the network, and control the IP packets passing the unauthorized proxy servers and IP packets transmitted to the unauthorized routers. Such control can prevent users from maliciously evading paying the fee for Internet access. At present, China Telecom, China Netcom, and other operators adopt ANTI-SNIPER to restrict Internet access sharing by users. ANTI-SNIPER can prevent the network access sharing behavior from being identified by operators.

6.2 Applications

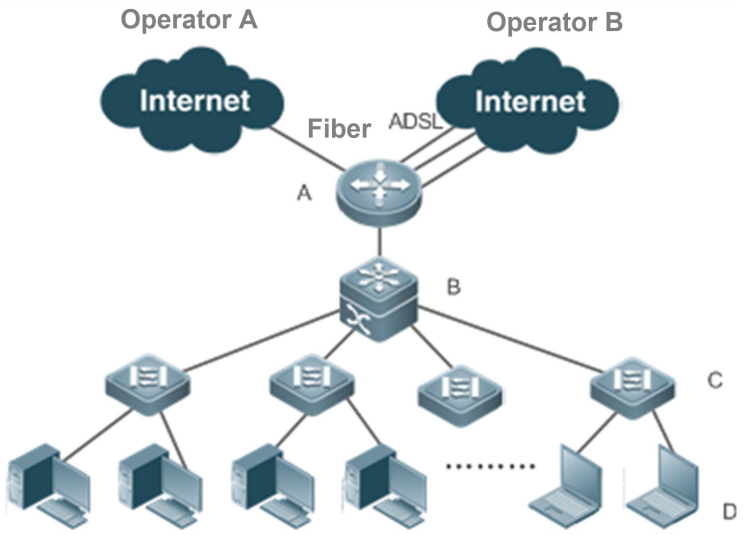
Application	Description
Deploying Egress Gateway	Deploys ANTI-SNIPER on an egress gateway.

6.2.1 Deploying Egress Gateway

Scenario

ANTI-SNIPER is usually deployed on a dial-up interface. Figure 6-1 shows the typical topology for a NetBar.

Figure 6-1 Typical Application Scenario for NetBar



Remarks	A indicates an egress gateway. B indicates a core switch. C indicates access switches. D indicates intranet clients.

Deployment

- Basic NAT: Implement basic network address translation (NAT) to ensure that clients access the Internet normally.
- Application identification: Identify the application for traffic forwarding.

- Application routing (including application proxy): Enable traffic of heavy-traffic applications or key applications to be transmitted via specified egress ports based on application identification.
- Flow control: Implement functions such as traffic guarantee of key applications in combination with application identification.
- L2/L3 application identification: Identify clients and client groups for traffic forwarding.
- Multilink load balancing: Distribute data flows to multiple links to ensure proper utilization of bandwidth.
- Flow audit: Count different types of traffic passing the gateway device based on clients or applications, to visualize the network traffic.
- ANTI-SNIPER: Prevent NetSniper of operators from identifying the network access sharing behavior.

6.3 Features

Overview

Feature	Description
ANTI-SNIPER	Enables this function to prevent NetSniper of operators from identifying the network access sharing behavior.

6.3.1 ANTI-SNIPER

ANTI-SNIPER prevents NetSniper of operators from identifying network access sharing and therefore restricting Internet access.

Working Principle

ANTI-SNIPER disguise clients by modifying the field values of packets, including the TTL, IPID, TCP port, window size, timestamp, and so on, so that behaviors of different clients appear to be generated by the same client. In addition, it splits HTTP packets to raise the difficulty for NetSniper of operators in auditing the packets, thereby avoiding the detection of Internet access sharing.

Related Configuration

Enabling ANTI-SNIPER

ANTI-SNIPER is disabled by default.

Run the **anti-sniper interface** *intf-name* command in global configuration mode to enable ANTI-SNIPER on a certain interface.

Run the **no anti-sniper interface** *intf-name* command in global configuration mode to disable ANTI-SNIPER on a certain interface.

Configuring TTL of IP Packet

The IP packet TTL modification function is enabled by default. The default TTL is 128.

Run the **ip-ttl off** command in ANTI-SNIPER mode to disable the IP packet TTL modification function. Run the **no ip-ttl off** command to enable the IP packet TTL modification function.

Run the **ip-ttl value** *num* command in ANTI-SNIPER mode to modify the TTL of IP packets. The value range of TTL is 1–255.

Run the **no ip-ttl value** command to restore the default TTL of IP packets.

This function is supported on the EG series and NBR series products.

Configuring IP Packet IPID Modification Mode

The IP packet IPID modification function is enabled by default. The default IPID modification mode is the ascending mode.

Run the **ip-id off** command in ANTI-SNIPER mode to disable the IP packet IPID modification function. Run the **no ip-id off** command in ANTI-SNIPER mode to enable this function.

Run the **ip-id random** command in ANTI-SNIPER mode to change the IPID modification mode to the random mode. Run the **no ip-id random** command in ANTI-SNIPER mode to restore the ascending mode.

This function is supported on the EG series and NBR series products.

Configuring TCP Port Modification Function

The TCP port modification function is disabled by default. Odd and even port IDs appear alternately. The port ID range is 1054–9000.

Run the **tcp-port off** command in ANTI-SNIPER mode to disable the TCP port modification function. Run the **no tcp-port off** command in ANTI-SNIPER mode to enable this function.

Run the **no tcp-port continuous** command in ANTI-SNIPER mode to adopt the ascending mode for port IDs. Run the **tcp-port continuous** command in ANTI-SNIPER mode to restore the default configuration.

Run the **tcp-port range** *port1 port2* command in ANTI-SNIPER mode to configure the port ID range. Run the **no tcp-port range** command in ANTI-SNIPER mode to restore the default configuration.

This function is supported on the EG series and NBR series products.

Configuring TCP Window Size Modification Function

The TCP window size modification function is enabled by default. The default window size is 65535.

Run the **tcp-win-size off** command in ANTI-SNIPER mode to disable this function. Run the **no tcp-win-size off** command in ANTI-SNIPER mode to enable this function.

Run the **tcp-win-size value** *num* command in ANTI-SNIPER mode to configure the window size, which ranges from **1** to **65535**. Run the **no tcp-win-size value** command in ANTI-SNIPER mode to restore the default configuration.

This function is supported on the EG series and NBR series products.

Configuring Packet Timestamp Removal Function

The packet timestamp removal function is enabled by default.

Run the **tcp-timestamp off** command in ANTI-SNIPER mode to disable this function. Run the **no tcp-timestamp off** command in ANTI-SNIPER mode to enable this function.

This function is supported on the EG series and NBR series products.

Configuring HTTP Packet Splitting Function

The HTTP packet splitting function is enabled by default. Splitting Mode 1 is adopted by default.

Run the **http-modify off** command in ANTI-SNIPER mode to disable this function. Run the **no http-modify off** command in ANTI-SNIPER mode to enable this function.

Run the **http-modify mode** *num* command in ANTI-SNIPER mode to change the splitting mode. Run the **no http-modify mode** command in ANTI-SNIPER mode to restore the default configuration.

This function is supported on the EG series and NBR series products.

6.4 Configuration

Configuration	Description and Command	
Enabling ANTI-SNIPER	(Mandatory) It is used to enable traffic audit.	
	anti-sniper interface *intf-name*	Enables traffic monitoring and audit.
Configuring TTL of IP Packet	(Optional) It is used to configure the TTL of an IP packet.	
	(no) ip-ttl off	Enables or disables the IP packet TTL modification function.
	ip-ttl *num*	Modifies the TTL of an IP packet.
Configuring IP Packet IPID Modification Mode	(Optional) It is used to modify the IPID of an IP packet.	
	(no) ip-id off	Enables or disables the IP packet IPID modification function.
	(no) ip-id random	Configures the IPID mode as ascending mode or random mode.
Configuring TCP Port Modification Function	(Optional) It is used to configure the TCP port modification function.	
	(no)tcp-port	Enables or disables the TCP port modification function.
	(no)tcp-port continuous	Sets the TCP port modification mode to ascending mode or odd-even alteration mode.
	tcp-port range *min-port max-port*	Configures the available TCP port range.
Configuring TCP Window Size Modification Function	(Optional) It is used to configure the TCP window size modification function.	
	(no) tcp-win-size off	Enables or disables TCP window size modification function.
	tcp-win-size *value*	Configures the TCP window size.
Configuring Timestamp Removal Function	(Optional) It is used to enable the packet timestamp removal function.	
	(no) tcp-timestamp off	Enables or disables the packet timestamp removal function.
Configuring HTTP Packet Splitting Function	(Optional) It is used to configure the HTTP packet splitting function.	
	(no)http-modify off	Enables or disables the HTTP packet splitting function.
	http-modify mode *value*	Configures the HTTP packet splitting mode.

6.4.1 Enabling ANTI-SNIPER

Configuration Effect

- Enable ANTI-SNIPER to prevent the network access sharing behavior from being identified by operators.

Notes

- The ANTI-SNIPER function is invalid when the ANTI-SNIPER switch is disabled.

Configuration Steps

- Run the **anti-sniper interface** *intf-name* command in global configuration mode to enable ANTI-SNIPER.

Verification

- Check the configuration information of ANTI-SNIPER.

Related Commands

Enabling ANTI-SNIPER on Interface

Command	**anti-sniper interface**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Enabling ANTI-SNIPER

Configuration Steps	Enable ANTI-SNIPER on Interface GI0/5 of an egress gateway device.
	FS# configure terminal FS(config)# anti-sniper interface gigabitEthernet 0/5
Verification	• Check the status of ANTI-SNIPER.
	FS#show anti-sniper policy [GigabitEthernet 0/5]

6.4.2 Configuring TTL of IP Packet

Configuration Effect

- Configure the IP packet TTL modification function and set the TTL.

Notes

- Optional.
- The IP packet TTL modification function is enabled by default. The default TTL is 128. The value range is 1–255.

Configuration Steps

- Run the commands in ANTI-SNIPER mode to enable or disable the IP packet TTL modification function and set the TTL.

Verification

- Check the status of the IP packet TTL modification function and check the TTL.

Related Commands

Enabling the IP Packet TTL Modification Function

Command	**no ip-ttl off**
Parameter Description	N/A
Command Mode	ANTI-SNIPER mode
Usage Guide	Run the **ip-ttl off** command to disable this function.

Modifying TTL

Command	**ip-ttl** *num*
Parameter Description	*num*: Indicates the TTL. The value range is 1–255.
Command Mode	ANTI-SNIPER mode
Usage Guide	If the IP packet TTL modification function is disabled, the configuration is invalid.

Configuration Example

Configuring the IP Packet TTL Modification Function and Setting TTL to 129

Configuration Steps	Configure the IP packet TTL modification function and set the TTL to **129** on the egress gateway device.
	FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# anti-sniper interface gigabitEthernet 0/5 FS(config-anti-sniper)#no ip-ttl off FS(config-anti-sniper)#ip-ttl 129
Verification	● Check the configuration information.
	FS(config)#show anti-sniper policy [GigabitEthernet 0/5] ip-ttl : ON ip-ttl value : 129

6.4.3 Configuring IP Packet IPID Modification Mode

Configuration Effect

- Configure the IP packet IPID modification mode.

Configuration Steps

- Run the commands in ANTI-SNIPER mode to enable or disable the IP packet IPID modification function and set the IPID modification mode.

Verification

- Check whether the function is enabled or disabled and check the modification mode.

Related Commands

Enabling IPID Modification Function

Command	**no ip-id off**
Parameter Description	N/A
Command Mode	ANTI-SNIPER mode
Usage Guide	N/A

Configuring IPID Modification Mode as Random Mode

Command	**ip-id random**
Parameter Description	N/A
Command Mode	ANTI-SNIPER mode
Usage Guide	N/A

Configuration Example

Enabling IPID Modification and Configuring IPID Modification Mode as Ascending Mode

Configuration Steps	Enable IPID modification and configure IPID modification mode as ascending mode on the egress gateway device.
	FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# anti-sniper interface gigabitEthernet 0/5 FS(config-anti-sniper)#no ip-id off FS(config-anti-sniper)# no ip-id random
Verification	● Check the configuration information.
	FS(config)#show anti-sniper policy [GigabitEthernet 0/5] ip-ttl : ON ip-ttl value : 129 ip-id : ON ip-id random : FALSE

6.4.4 Configuring TCP Port Modification Function

Configuration Effect

- Configure the TCP port modification function and designate the port range and modification mode.

Configuration Steps

- Run the commands in ANTI-SNIPER mode to enable or disable the TCP port modification function and set the modification mode and the port range.

Verification

- Check the configuration information.

Related Commands

Enabling TCP Port Modification Function

Command	**no tcp-port off**
Parameter Description	N/A
Command Mode	ANTI-SNIPER mode
Usage Guide	N/A

Configuring TCP Port Modification Mode as Ascending Mode

Command	**tcp-port continuous**
Parameter Description	N/A
Command Mode	ANTI-SNIPER mode
Usage Guide	N/A

Configuring TCP Port Range

Command	**tcp-port range** *min-port max-port*
Parameter Description	*min-port*: Indicates the minimum value in the port range. The port range is 1–65535. The default value is **1054**. *max-port*: Indicates the maximum value in the port range. The port range is 1–65535. The default value is **9000**.
Command Mode	ANTI-SNIPER mode
Usage Guide	N/A

Configuration Example

Enabling TCP Port Modification Function, Configuring TCP Port Modification Mode as Ascending Mode, and Setting Port Range to 2000–8000

Configuration Steps	Enable TCP port modification function, configure TCP port modification mode as ascending mode, and set the port range to 2000–8000 on the egress gateway device.
	FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# anti-sniper interface gigabitEthernet 0/5 FS(config-anti-sniper)#no tcp-port off FS(config-anti-sniper)#tcp-port continuous FS(config-anti-sniper)# tcp-port range 2000 8000
Verification	● Check the configuration information.
	FS(config-anti-sniper)#show anti-sniper policy [GigabitEthernet 0/5] ip-ttl : ON ip-ttl value : 128 ip-id : ON ip-id random : TRUE tcp-port : ON tcp-port continuous : TRUE tcp-port range : 2000-8000

6.4.5 Configuring TCP Window Size Modification Function

Configuration Effect

- Configure the TCP window size modification function and set the window size.

Notes

- The TCP window size modification function is enabled by default. The default window size is 65535.

Verification

- Check the configuration information.

Related Commands

Enabling TCP Window Size Modification Function

Command	**no tcp-win-size off**
Parameter Description	N/A
Command Mode	ANTI-SNIPER mode
Usage Guide	N/A

Setting Window Size

Command	**tcp-win-size** *value*
Parameter Description	*value*: Indicates the window size. The value range is from 1 to 65535. The default value is **65535**.
Command Mode	ANTI-SNIPER mode
Usage Guide	N/A

Configuration Example

Enabling TCP Window Size Modification Function and Setting Window Size to 65535

Configuration Steps	Enable the TCP window size modification function and set the window size to **65535** on the egress gateway device.
	FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# anti-sniper interface gigabitEthernet 0/5 FS(config-anti-sniper)#no tcp-win-size off FS(config-anti-sniper)# tcp-win value 65535
Verification	● Check the configuration information.
	FS(config-anti-sniper)#show anti-sniper policy [GigabitEthernet 0/5] ip-ttl : ON ip-ttl value : 128 ip-id : ON ip-id random : TRUE tcp-port : ON tcp-port continuous : TRUE tcp-port range : 2000-8000 tcp-win-size : ON tcp-win-size value : 65535

6.4.6 Configuring Timestamp Removal Function

Configuration Effect

- Configure the packet timestamp removal function.

Notes

- The packet timestamp removal function is enabled by default.

Verification

- Check the configuration information.

Related Commands

Enabling Packet Timestamp Removal Function

Command	**no tcp-timestamp off**
Parameter Description	N/A
Command Mode	ANTI-SNIPER mode
Usage Guide	N/A

Configuration Example

Enabling Packet Timestamp Removal Function

Configuration Steps	Enable the packet timestamp removal function on the egress gateway device.
	FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# anti-sniper interface gigabitEthernet 0/5 FS(config-anti-sniper)#no tcp-timestamp off
Verification	● Check the configuration information.
	FS(config-anti-sniper)#show anti-sniper policy [GigabitEthernet 0/5] ip-ttl : ON ip-ttl value : 128 ip-id : ON ip-id random : TRUE tcp-port : ON tcp-port continuous : TRUE tcp-port range : 2000-8000 tcp-win-size : ON tcp-win-size value : 65535 tcp-timestamp : ON

6.4.7 Configuring HTTP Packet Splitting Function

Configuration Effect

- Configure the HTTP packet splitting function and set the splitting mode.

Notes

- Optional.
- The HTTP packet splitting function is enabled by default. The default splitting mode is Mode 1.

Configuration Steps

- Run the commands in ANTI-SNIPER mode to enable or disable the HTTP packet splitting function and set the splitting mode.

Verification

- Check the configuration information.

Related Commands

Enabling HTTP Packet Splitting Function

Command	**no http-modify off**
Parameter Description	N/A
Command Mode	ANTI-SNIPER mode
Usage Guide	N/A

Configuring the HTTP Packet Splitting Mode

Command	**http-modify mode** *num*
Parameter Description	*num*: Indicates the HTTP packet splitting mode. The value range is 1–4. The default value is **1**.
Command Mode	ANTI-SNIPER mode
Usage Guide	If the switch of **http-modify** is disabled, this function is invalid.

Configuration Example

Enabling HTTP Packet Splitting Function and Setting Splitting Mode to Mode 1

Configuration Steps	Enable HTTP packet splitting function and set the splitting mode to Mode 1 on the egress gateway device.
	FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# anti-sniper interface gigabitEthernet 0/5 FS(config-anti-sniper)#no http-modify off FS(config-anti-sniper)# http-modify mode 1
Verification	● Check the configuration information.

```
FS(config-anti-sniper)#show anti-sniper policy
[GigabitEthernet 0/5]
ip-ttl                    : ON
ip-ttl value              : 128
ip-id                     : ON
ip-id random              : TRUE
tcp-port                  : ON
tcp-port continuous       : TRUE
tcp-port range            : 2000-8000
tcp-win-size              : ON
tcp-win-size value        : 65535
tcp-timestamp             : ON
http-modify               : ON
http-modify mode          : 1
```

6.5 Monitoring

Displaying

Description	Command
Displays the current configuration information.	**show anti-sniper policy**

Debugging

Description	Command
Displays whether the kernel configuration is synchronized.	**show anti-sniper ef-policy**
Displays the running status of the kernel.	**show anti-sniper stat**

Chapter 9 Reliability Configuration

1. Configuring VRRP
2. Configuring RNS

1 Configuring VRRP

1.1 Overview

Virtual Router Redundancy Protocol (VRRP) is a fault-tolerant routing protocol.

VRRP adopts the master-backup design to ensure migration of functions from a Master router to a Backup one when the Master failed, without influencing internal and external data communication or modifying Local Area Network (LAN) configuration. A VRRP group maps multiple routers into a virtual router. VRRP ensures only one router at a moment on behalf of a virtual router transfers packets, which is the elected Master. If the Master fails, one of the Backup routers will replace it. Under VRRP, it seems that a host in a LAN uses only one router and the routing remains functional even when the first-hop router fails.

- VRRP is applicable to LAN scenarios which require the redundancy of routing egresses.

Protocols and Standards

- RFC2338: Virtual Router Redundancy Protocol
- RFC3768: Virtual Router Redundancy Protocol (VRRP)
- RFC5798: Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4

1.2 Applications

Application	Description
Routing Redundancy	Configure routers in a LAN as one VRRP group to achieve simple routing redundancy.
Load Balancing	Configure routers in a LAN as multiple VRRP groups to achieve traffic load balancing.

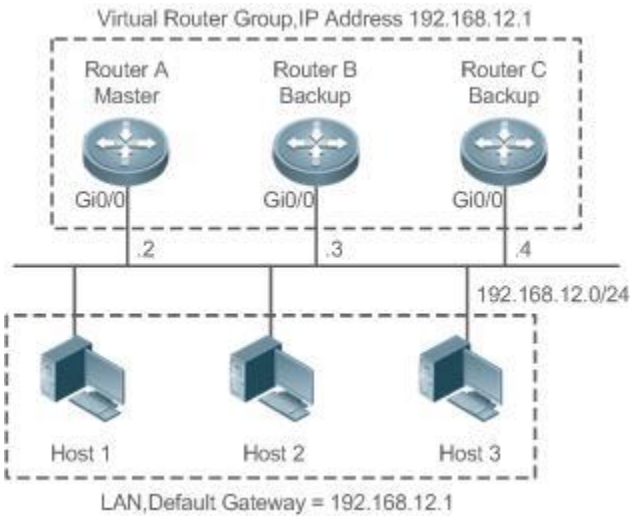
1.2.1 Routing Redundancy

Scenario

Configure routers in a LAN as one VRRP group, where hosts take the virtual IP address of this group as the default gateway address.

- Packets from Host 1, Host 2 and Host 3 to other networks are forwarded by the elected Master router (Router A in Figure 1- 1).
- If Router A fails, the Master will be re-elected between Router B and Router C to forward packets, achieving simple routing redundancy.

Figure 1- 1



Deployment

- Router A, Router B and Router C are connected to the LAN via Ethernet interfaces.
- On Router A, Router B and Router C, VRRP is configured on the Ethernet interfaces connected to the LAN.
- These Ethernet interfaces are in the same VRRP group whose virtual IP address is 192.168.12.1.
- The gateway address for Host 1, Host 2 and Host 3 is the IP address of the VRRP group, namely 192.168.12.1.

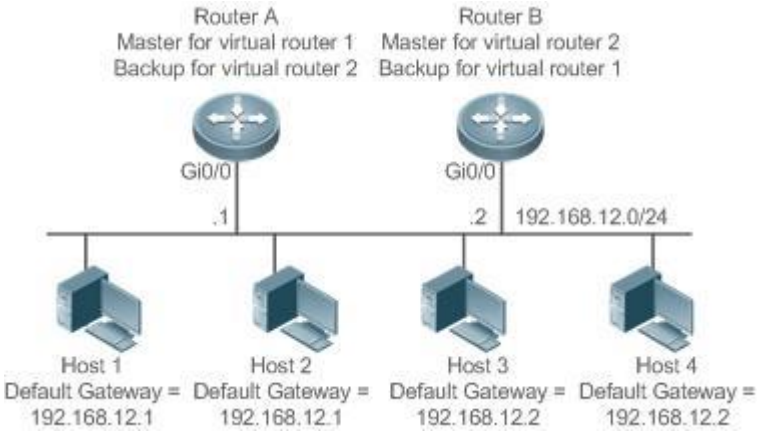
1.2.2 Load Balancing

Scenario

Configure routers in a LAN as multiple VRRP groups. Hosts in the LAN take virtual IP addresses of the groups as their gateways, and each router backs up for other routers in different group.

- Packets from Host 1 and Host 2 to other networks with the default gateway address as the virtual IP address of virtual router 1 are forwarded by the Master of virtual router 1 (Router A in Figure 1- 2).
- Packets from Host 3 and Host 4 to other networks with the default gateway address as the virtual IP address of virtual router 2 are forwarded by the Master of virtual router 2 (Router B in Figure 1- 2).
- Routing redundancy is achieved on Router A and Router B, and the LAN traffic is shared to achieve load balancing.

Figure 1- 2



Deployment

- Router A and Router B are connected to the LAN via Ethernet interfaces.
- On Router A and Router B, two virtual routers are configured on the Ethernet interfaces connected to the LAN.

Router A takes the IP address 192.168.12.1 of Ethernet interface Gi0/0 as the IP address of virtual router 1. Thus for virtual router 1, Router A becomes the Master and Router B becomes the Backup.

- Router B takes the IP address 192.168.12.2 of Ethernet interface Gi0/0 as the IP address of virtual router 2. Thus for virtual router 2, Router B becomes the Master and Router A becomes the Backup.
- In the LAN, Host 1 and Host 2 take the IP address 192.168.12.1 of virtual router 1 as the default gateway address, while Host 3 and Host 4 take the IP address 192.168.12.2 of virtual router 2 as the default gateway address.

1.3 Features

Basic Concepts

Virtual Router

A virtual router, also called a VRRP group, is regarded as a default gateway for hosts in a LAN. A VRRP group contains a Virtual Router Identifier (VRID) and a set of virtual IP addresses.

Virtual IP Address

Indicates the IP address of a virtual router. A virtual router can be configured with one or multiple IP addresses.

IP Address Owner

If a VRRP group has the virtual IP address as that of an Ethernet interface on one real router, the router is regarded as the virtual IP address owner. In such case, the router priority is 255. If the owned Ethernet interface is available, the VRRP group will be in Master state automatically. The IP address owner receives and processes the packets with the destination IP address as that of the virtual router.

Virtual MAC Address

The virtual MAC address of a VRRP group is an IEEE 802 MAC address, formatted as **00-00-5E-00-01-{VRID}** with the first five octets assigned and the last two as a group VRID. A VRRP group responds to an Address Resolution Protocol (ARP) request with its virtual MAC address instead of a real MAC address.

Master Router

In a VRRP group, only the Master router answers ARP requests and forwards IP packets. If a real router is the IP Address Owner, it becomes the Master router.

Backup Router

In a VRRP group, Backup routers only monitor the state of the Master but do not respond to ARP requests or forward IP packets. When the Master fails, Backup routers will take the chance to compete for the position.

Preemption Mode

If a VRRP group runs in Preemption mode, a higher priority Backup router will replace the lower priority Master router.

Overview

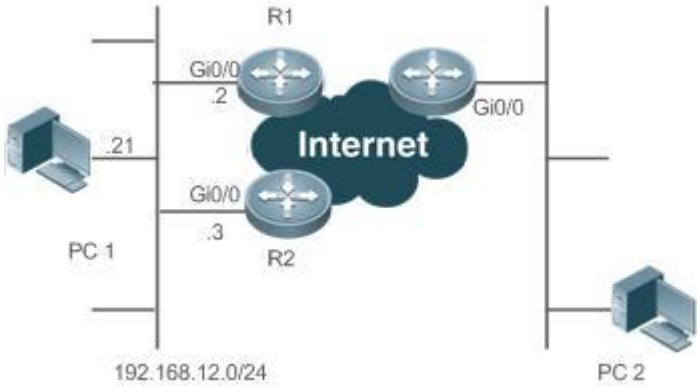
Feature	Description
VRRP	VRRP achieves redundancy for the default gateways of terminals on a multi-access media (for example, Ethernet). It enables a Backup router to forward packets when the Master router is down, providing transparent routing switch and promoting network service quality.

1.3.1 VRRP

In case that the Master router is faulty, VRRP achieves migration of functions from the Master router to a Backup one without influencing internal and external data communication or modifying LAN configuration.

Working Principle

Figure 1- 3 Working Principle of VRRP



Working Mode of VRRP

The RFC2338, RFC3768 and RFC5798 protocols define the format and operating mechanism of VRRP packets. Multicast VRRP packets are sent periodically with specified destination addresses by the Master router to advertise normal operation or for Master election. VRRP allows a router in a LAN to automatically replace the Master who forwards IP packets when the latter fails. This helps achieve hot backup and fault tolerance of IP-based routing as well as ensure communication continuity and reliability for hosts in the LAN. A VRRP group achieves redundancy through multiple real routers. However, only one router acts as the Master to forward packets while the others are Backup routers. Router switching in a VRRP group is completely transparent to hosts in a LAN.

Master Election Process

The RFC standards stipulate the master election process as follows:

- VRRP provides a simple mechanism for Master election. First, compare the VRRP priorities configured on the interfaces of the routers in a VRRP group. The router with the highest priority is elected as the Master. If these priorities are equal, compare the primary IP addresses of these routers. The router with the biggest IP address is elected as the Master.
- After the Master router is elected, the other routers become Backup routers (and enter the **Backup** state) and monitor the state of the master router through the VRRP packets the master router sends. If the master router is operational, it regularly sends VRRP multicast packets known as Advertisement packets to notify the Backup routers of its status. If the Backup routers do not receive such packets within a set period, all of them will enter the Master state. In such case, the previous step of Master election is repeated. In this way, a router with the highest priority will be elected as a new master, achieving VRRP backup.

Once the Master router of a VRRP group is elected, it is responsible to forward packets for hosts in a LAN.

Communication Process

The VRRP communication process can be explained by Figure 1-3. The routers R1 and R2 are connected to the LAN segment 192.168.12.0/24 via the VRRP-enabled Ethernet interfaces Gi0/0. Hosts in the LAN take the virtual IP address of the VRRP group as the default gateway address. Only the virtual router is recognized by the hosts. The Master router in the group, however, is unknown. For example, when PC 1 plan to communicate with PC 2, PC 1 sends packets to the default gateway with the virtual IP address; The Master router in the group receives the packets and forwards them to PC 2. In this process, PC 1 only senses the virtual router instead of R1 or R2. The Master router in the group is elected between R1 and R2. When the Master fails, it will be replaced automatically by the other router.

Related Configuration

Enabling VRRP

By default, VRRP is disabled on an interface.

In the interface configuration mode, run the **vrrp** *group* **ip** *ipaddress* [**secondary**] command to set the VRID and virtual IP address to enable VRRP.

VRRP must be enabled on an interface.

Configuring the IPv4 VRRP Authentication String

By default, VRRP is in non-authentication mode.

Run the **vrrp group authentication** *string* command to set an authentication string in MD5 authentication mode or a plain text password in plain text mode for an IPv4 VRRP group. In the plain text authentication mode, a password contains 8 bytes at most.

Members of a VRRP group can communicate with each other only when they are in the same authentication mode. In the plain text authentication mode, all routers in a VRRP group should have the same authentication password. The plain text authentication password cannot guarantee security but only prevents/prompts wrong VRRP configurations.

Configuring the VRRP Advertisement Interval

By default, the advertisement interval of the Master router is 1 second.

Run the **vrrp** *group* **timers advertise** *{ advertise-interval* | **csec** *centisecond-interval }* command to change the interval.

When VRRP learning timer is not configured, the same advertisement interval should be set for a VRRP group, otherwise routers in **Backup** state will discard received VRRP packets.

Configuring the VRRP Preemption Mode

By default, a VRRP group operates in the Preemption mode.

To enable the Preemption mode for a VRRP group, run the **vrrp** *group* **preempt** [**delay** *seconds*] command. The optional parameter **delay** *seconds* is 0 by default.

If a VRRP group operates in the Preemption mode, a router will become the Mater of the group when it finds that its priority is higher than that of the current Master. If a VRRP group operates in Non-preemption mode, a router will not become the Master even when it finds that its priority is higher than that of the current Master. It makes little sense to configure the Preemption mode when the VRRP group uses the IP address of an Ethernet interface, in which case the group has the highest priority and automatically becomes the Master in the group. The optional parameter **Delay** *Seconds* defines the delay before a backup VRRP router declares its Master identity.

Configuring the VRRP Router Priority

By default, the router priorities in a VRRP group are all 100.

To adjust the priority, run the **vrrp** *group* **priority** *level* command.

If a router in the Preemption mode owns the group's virtual IP address and the highest priority, it becomes the group Master, while the other routers with lower priorities in the group become Backup (or monitoring) routers.

Configuring the VRRP Tracked IP Address

By default, no IP address is tracked by a VRRP group.

To configure such an address, run the **vrrp** *group* **track** *ip-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]

After an IP address is configured for a VRRP group to monitor, the router priority will be adjusted dynamically based on the address accessibility. Once the address is inaccessible (the **ping** command fails), the priority of the router in the group will be reduced by a set value, and another higher priority router in this group will become the Master.

Configuring the VRRP Learning Timer

By default, the learning timer is disabled for a VRRP group.

To enable it, run the **vrrp** *group* **timers learn** command.

After the learning timer is configured, a VRRP Backup router learns the advertisement interval of NA packets from the Master. Based on this instead of a locally set interval, the Backup router calculates the interval for determining a failure of the Master. This command achieves the synchronization of advertisement intervals between Backup routers and the Master.

Configuring the VRRP Group Description

By default, no description is configured for a VRRP group.

To configure such a string, run the **vrrp** *group* **description** *text* command.

A VRRP description helps distinguishing VRRP groups. A description has 80 bytes at most, otherwise wrong configuration is prompted.

Configuring the VRRP Delay

By default, no delay is configured for a VRRP group.

To enable it, run the **vrrp delay** { **minimum** *min-seconds* | **reload** *reload-seconds* } command. The two types of delay range from 0 to 60 seconds.

The command configures the delay of starting a VRRP group on an interface. There are two types of VRRP delay: the delay after system startup and the delay after an interface resumes. You may configure them respectively or simultaneously. After the delay is configured for a VRRP group on an interface, the VRRP group starts after the delay instead of immediately upon system startup or the interface's resumption, ensuring non-preemption. If the interface receives a VRRP packet during the delay, the delay will be canceled and the VRRP will be started immediately.

Configuring the IPv4 VRRP Version

By default, IPv4 adopts the VRRPv2 standard.

To specify the version for IPv4 VRRP, run the **vrrp** *group* **version** { **2 | 3** } command.

When the parameter value is set to 2, VRRPv2 is adopted; when the parameter value is set to 3, VRRPv3 is adopted.

1.4 Configuration

Configuration	Description and Command	
Configuring IPv4 VRRP	(Mandatory) It is used to enable IPv4 VRRP.	
	vrrp *group* **ip** *ipaddress* [**secondary**]	Enables IPv4 VRRP.
	(Optional) It is used to configure IPv4 VRRP parameters.	
	vrrp *group* **authentication** *string*	Configures the IPv4 VRRP authentication string.
	vrrp *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }	Configures the IPv4 VRRP advertisement interval.
	vrrp *group* **preempt** [**delay** *seconds*]	Configures the IPv4 VRRP Preemption mode.
	vrrp *group* **priority** *level*	Configures the IPv4 VRRP router priority.
Configuring VRRP-MSTP	The configuration is the same as IPv4 VRRP configuration.	

1.4.1 Configuring IPv4 VRRP

Configuration Effect

- Configure a VRRP group on an interface of a specific LAN segment by setting the VRID and virtual IP address.
- Configure multiple VRRP groups on an interface to achieve load balancing and offer more stable and reliable network services.
- Configure the VRRP tracked interfaces to monitor real-time failures, change interface priorities and realize master-backup failover dynamically.

Notes

- To achieve VRRP, the routers in a VRRP group should be configured with the same virtual IPv4 address.
- To achieve mutual backup between multiple IPv4 VRRP groups, configure multiple IPv4 VRRP groups with identical VRRP configuration on different interface and configure different priorities for them so that they act as the master and backup groups mutually.
- Enable VRRP on Layer-3 interfaces.

Configuration Steps

Enabling IPv4 VRRP

- By default, IPv4 VRRP is disabled on an interface. You can enable it based on your demand.

Configuring the IPv4 VRRP Authentication String

- By default, VRRP is in non-authentication mode. You can enable plain text authentication mode based on your demand.

Configuring the IPv4 VRRP Advertisement Interval

- By default, the Master router sends advertisement packets every one second. You can modify the interval based on your demand.

Configuring the IPv4 VRRP Preemption Mode

- By default, a VRRP group operates in Preemption mode with a zero-second delay.

Configuring the IPv4 VRRP Router Priority

- The default router priority for a VRRP group is 100. You can modify the priority based on your demand.

Configuring the IPv4 VRRP Tracked Interface

- By default, an IPv4 VRRP group monitors no interface and the value of priority change is 10. To achieve fault monitoring through interface monitoring, please configure this item.

Configuring the IPv4 VRRP Learning Timer

- By default, the learning timer is disabled for a VRRP group. Enable this function if the Backup routers need to learn the Master's advertisement interval.

Configuring the IPv4 VRRP Group Description

- By default, no description is configured for a VRRP group. To distinguish VRRP groups clearly, configure descriptions.

Configuring the IPv4 VRRP Delay

- By default, the IPv6 VRRP delay is not configured. To guarantee an effective non-preemption mode, configure the delay.

Configuring the IPv4 VRRP Version

- By default, IPv4 adopts the VRRPv2 standard. To change it, use the corresponding command.

Verification

- Run the **show vrrp** command to verify the configuration.

Related Commands

Enabling IPv4 VRRP

Command	**vrrp** *group* **ip** *ipaddress* [**secondary**]
Parameter Description	*group*: Indicates the VRID of a VRRP group, the range of which varies with product models. *ipaddress*: Indicates the IP address of a VRRP group. **secondary**: Indicates the secondary IP address of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	If no virtual IP address is specified, routers cannot join a VRRP group. If no secondary IP address is applied, the configured IP address will be the primary IP address of a VRRP group.

Configuring the IPv4 VRRP Authentication String

Command	**vrrp** *group* **authentication** *string*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *string*: Indicates the authentication string of a VRRP group (a plain text password consists of 8 bytes at most).
Command Mode	Interface configuration mode
Usage Guide	In a VRRP group, the same authentication password should be configured for routers. The plain text authentication

	password cannot guarantee security but only prevents/prompts wrong VRRP configurations.

Configuring the IPv4 VRRP Advertisement Interval

Command	**vrrp** *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }
Parameter Description	*group*: Indicates the VRID of a VRRP group. *advertise-interval*: Indicates the advertisement interval of a VRRP group (unit: second). ***csec*** *centisecond-interval:* An interval for a master router in a backup group to send VRRP packets. It is an integer from 50 to 99. The unit is centisecond. No default value is provided. If it is configured for VRRPv2 packets, the default interval is one second.
Command Mode	Interface configuration mode
Usage Guide	If a router is elected as the Master in a VRRP group, it sends VRRP advertisement packets at the set interval to announce its VRRP state, priority and other information.

Configuring the IPv4 VRRP Preemption Mode

Command	**vrrp** *group* **preempt** [**delay** *seconds*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. **delay** *seconds*: Indicates the preemption delay for the Master router to claim its status. The default value is 0 second.
Command Mode	Interface configuration mode
Usage Guide	If a VRRP group runs in Preemption mode, a higher priority router will take the place of the lower priority Master. If a VRRP group runs in Non-preemption mode, a router with the priority higher than that of the Master remains Backup. It makes little sense to configure the Preemption mode when the VRRP group uses the IP address of an Ethernet interface, in which case the group has the highest priority and automatically becomes the Master in the group.

Configuring the IPv4 VRRP Router Priority

Command	**vrrp** *group* **priority** *level*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *level*: Indicates the priority of an interface in a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	This command is used to manually configure the VRRP router priority.

Configuring the IPv4 VRRP Tracked Interface

Command	**vrrp** *group* **track** *interface-type interface-number* [*priority*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. *interface-type interface-number*: Indicates the interface to be tracked. *priority*: Indicates the scale of VRRP priority change when the state of a monitored interface changes. The default value is 10.
Command Mode	Interface configuration mode
Usage Guide	A tracked interface must be a routable Layer-3 logic interface (for example, a Routed port, an SVI interface, and a Loopback interface).

	The priority of the router owns the virtual IP address associated with a VRRP group must be 255, and no tracked interface can be configured on it.

Configuring the IPv4 VRRP Tracked IP Address

Command	**vrrp** *group* **track** *ipv4-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. *ipv4-addres*: Indicates the IPv4 address to be tracked. **interval** *interval-value*: Indicates the probe interval. The unit is second. Unless configured manually, the value is 3 seconds by default. **timeout** *timeout-value*: Indicates the probe timeout of waiting for responses. If no response is received when the timeout is up, it is regarded that the destination is inaccessible. The unit is second. Unless configured manually, the value is 1 second by default. **retry** *retry-value*: Indicates the probe retries. If the probe packet is sent continually for retry-value times but no response is received, it is regarded that the destination is inaccessible. The unit is times. Unless configured, the value is 3 times by default. *priority*: Indicates the scale of VRRP priority change when the state of a monitored interface changes. The default value is 10.
Command Mode	Interface configuration mode
Usage Guide	To monitor a host, specify its IPv4 address for an IPv4 VRRP group. If a VRRP group owns the actual IP address of an Ethernet interface, the group priority is 255, and no monitored IP address can be configured.

Configuring the IPv4 VRRP Learning Timer

Command	**vrrp** *group* **timers learn**
Parameter Description	*group*: Indicates the VRID of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	Once the learning timer is enabled on a VRRP router, a Backup router learns the advertisement interval of the Master during the timer. Based on this, the Backup router calculates the interval for determining the Master router as failed instead of using the locally configured advertisement interval. This command achieves synchronization with the learning timer between the Master and Backup routers.

Configuring the IPv4 VRRP Group Description

Command	**vrrp** *group* **description** *text*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *text*: Indicates the description of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	A VRRP description helps distinguishing VRRP groups. A description has 80 bytes at most, otherwise wrong configuration is prompted.

Configuring the IPv4 VRRP Delay

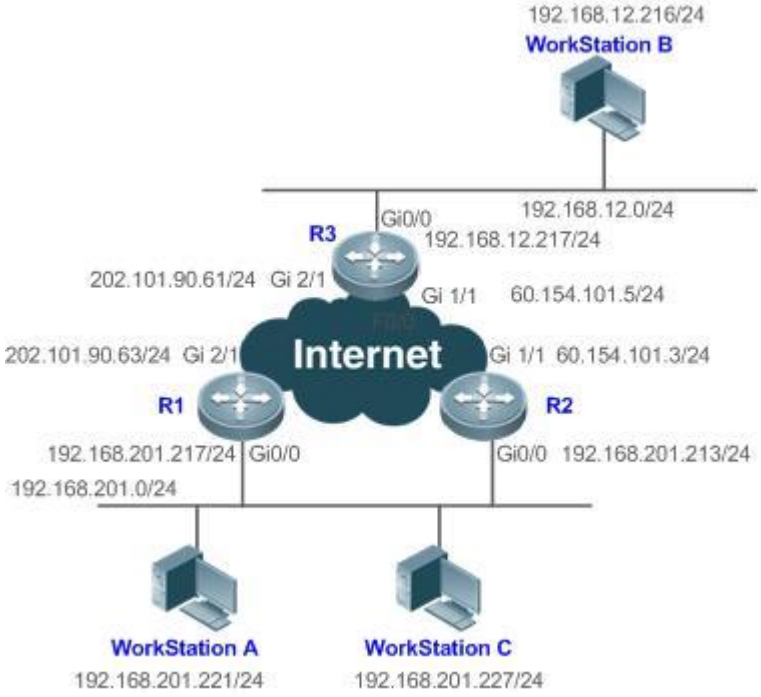
Command	**vrrp delay** { **minimum** *min-seconds* | **reload** *reload-seconds* }
Parameter Description	**minimum** *min-seconds*: Indicates the VRRP delay after an interface state changes. **reload** *reload-seconds*: Indicates the VRRP delay after the system starts.
Command Mode	Interface configuration mode
Usage Guide	After the delay is configured for a VRRP group on an interface, the VRRP group starts after the delay instead of immediately upon system startup or the interface's resumption, ensuring non-preemption. If the interface receives a VRRP packet during the delay, the delay will be canceled and the VRRP will be started immediately. The two types of delay share a value range of 0 to 60 seconds.

Configuring the IPv4 VRRP Version

Command	**vrrp** *group* **version** { **2** | **3** }
Parameter Description	**2**: Indicates VRRPv2. **3**: Indicates VRRPv3.
Command Mode	Interface configuration mode
Usage Guide	Considering the compatibility between VRRPv2 and VRRPv3, specify a standard for IPv4 VRRP based on the actual network condition. VRRPv2 is developed in RFC3768, while VRRPv3 is described in RFC5798. This command is only applicable to IPv4 VRRP.

Configuration Example

Configuring an IPv4 VRRP Group and Tracked Interface

Scenario **Figure 1- 4**	
Configuration Steps	● The cluster of Work Station A and Work Station B (192.168.201.0/24) uses the virtual IP address 192.168.201.1 of the VRRP group constituted by the routers R1 and R2 as the gateway address to communicate with Work Station B (192.168.12.0 /24).

	● GigabitEthernet 2/1 on R1 is configured as the tracked interface. ● No VRRP but an ordinary routing function is configured on R3.
R3	R3#configure terminal R3(config)#interface GigabitEthernet 0/0 // The command “no switchport” is only required for a switch. R3(config-if-GigabitEthernet 0/0)#no switchport R3(config-if-GigabitEthernet 0/0)#ip address 192.168.12.217 255.255.255.0 R3(config-if-GigabitEthernet 0/0)#exit R3(config)#interface GigabitEthernet 1/1 // The command “no switchport” is only required for a switch. R3(config-if-GigabitEthernet 1/1)#no switchport R3(config-if-GigabitEthernet 1/1)#ip address 60.154.101.5 255.255.255.0 R3(config-if-GigabitEthernet 1/1)#exit R3(config)#interface GigabitEthernet 2/1 // The command “no switchport” is only required for a switch. R3(config-if-GigabitEthernet 2/1)#no switchport R3(config-if-GigabitEthernet 2/1)#ip address 202.101.90.61 255.255.255.0 R3(config-if-GigabitEthernet 2/1)#exit R3(config)#router ospf R3(config-router)#network 202.101.90.0 0.0.0.255 area 10 R3(config-router)#network 192.168.12.0 0.0.0.255 area 10 R3(config-router)#network 60.154.101.0 0.0.0.255 area 10
R1	R1#configure terminal R1(config)#interface GigabitEthernet 0/0 R1(config-if-GigabitEthernet 0/0)#ip address 192.168.201.217 255.255.255.0 R1(config-if-GigabitEthernet 0/0)#vrrp 1 priority 120 R1(config-if-GigabitEthernet 0/0)#vrrp 1 version 3 R1(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise 3 R1(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.201.1 R1(config-if-GigabitEthernet 0/0)#vrrp 1 track GigabitEthernet 2/1 30 R1(config-if-GigabitEthernet 0/0)#exit R1(config)#interface GigabitEthernet 2/1 R1(config-if-GigabitEthernet 2/1)#ip address 202.101.90.63 255.255.255.0 R1(config-if-GigabitEthernet 2/1)#exit

	R1(config)#router ospf R1(config-router)#network 202.101.90.0 0.0.0.255 area 10 R1(config-router)#network 192.168.201.0 0.0.0.255 area 10
R2	R2#configure terminal R2(config)#interface GigabitEthernet 0/0 R2(config-if-GigabitEthernet 0/0)#ip address 192.168.201.213 255.255.255.0 R2(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.201.1 R2(config-if-GigabitEthernet 0/0)#vrrp 1 version 3 R2(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise 3 R2(config-if-GigabitEthernet 0/0)#exit R2(config)#interface GigabitEthernet 1/1 // The command “no switchport” is only required for a switch. R2(config-if-GigabitEthernet 1/1)#no switchport R2(config-if-GigabitEthernet 1/1)#ip address 60.154.101.3 255.255.255.0 R2(config-if-GigabitEthernet 1/1)#exit R2(config)#router ospf R2(config-router)#network 60.154.101.0 0.0.0.255 area 10 R2(config-router)#network 192.168.201.0 0.0.0.255 area 10
Verification	Run the **show vrrp** command to verify the configuration. ● Check whether R1, which acts as the Master, reduces its VRRP priority from 120 to 90 when GigabitEthernet2/1 connected to the Wide Area Network (WAN) is unavailable. If yes, R2 becomes the Master. ● Check whether R1 resumes its VRRP priority from 30 to 120 when GigabitEthernet 2/1 connected to the WAN recovers. If yes, R1 is re-elected as the Master.
R1	R1#show vrrp GigabitEthernet 0/0 - Group 1 State is Master Virtual IP address is 192.168.201.1 configured Virtual MAC address is 0000.5e00.0101 Advertisement interval is 3 sec Preemption is enabled min delay is 0 sec Priority is 120 Master Router is 192.168.201.217 (local), priority is 120 Master Down interval is 10.59 sec

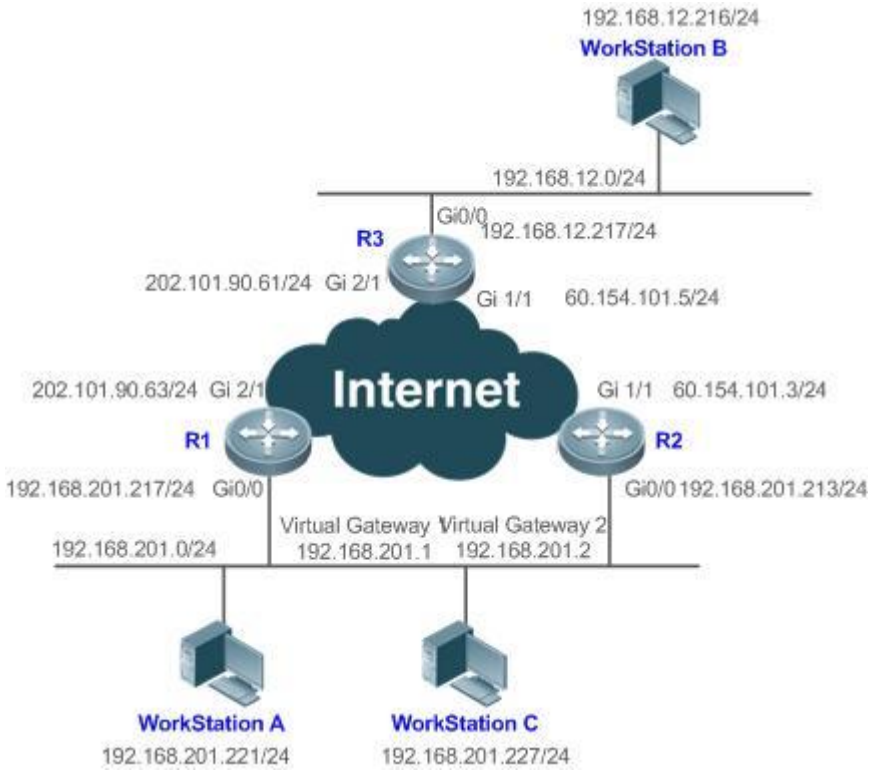
	Tracking state of 1 interface, 1 up: up GigabitEthernet 2/1 priority decrement=30
R2	R2#show vrrp GigabitEthernet 0/0 - Group 1 State is Backup Virtual IP address is 192.168.201.1 configured Virtual MAC address is 0000.5e00.0101 Advertisement interval is 3 sec Preemption is enabled min delay is 0 sec Priority is 100 Master Router is 192.168.201.217 , priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.82 sec

Common Errors

- Different virtual IP addresses are configured on the routers in a VRRP group, resulting in multiple Master routers in the group.
- Different VRRP advertisement intervals are configured on the routers in a VRRP group and the learning timer is not configured, resulting in multiple Master routers in the group.
- Different VRRP versions are configured on the routers in a VRRP group, resulting in multiple Master routers in the group.
- For VRRPv2, the Ethernet interfaces of the routers in a VRRP group are all in plain text authentication mode but inconsistent in authentication strings, resulting in multiple Master routers in the group.

Configuration Example

Configuring Multiple IPv4 VRRP Groups

Scenario Figure 1- 5	
Configuration Steps	● The user workstation cluster (192.168.201.0/24) uses the backup group constituted by the routers R1 and R2. The gateway for partial workstations (A for example) points to the virtual IP address 192.168.201.1 of the backup group 1, while that for other partial workstations (C for example) points to the virtual IP address 192.168.201.2 of the backup group 2. IPv4 multicast routing is enabled on all the routers. ● R1 acts as the master router in the group 2 and as a backup router in the group 1. ● R2 acts as a backup router in the group 2 and as a master router in the group 1.
R3	R3#configure terminal R3(config)#interface GigabitEthernet 0/0 // The command “no switchport” is only required for a switch. R3(config-if-GigabitEthernet 0/0)#no switchport R3(config-if-GigabitEthernet 0/0)#ip address 192.168.12.217 255.255.255.0 R3(config-if-GigabitEthernet 0/0)#exit R3(config)#interface GigabitEthernet 1/1 // The command “no switchport” is only required for a switch. R3(config-if-GigabitEthernet 1/1)#no switchport R3(config-if-GigabitEthernet 1/1)#ip address 60.154.101.5 255.255.255.0 R3(config-if-GigabitEthernet 1/1)#exit R3(config)#interface GigabitEthernet 2/1 // The command “no switchport” is only required for a switch.

	R3(config-if-GigabitEthernet 2/1)#no switchport R3(config-if-GigabitEthernet 2/1)#ip address 202.101.90.61 255.255.255.0 R3(config-if-GigabitEthernet 2/1)#exit R3(config)#router ospf R3(config-router)#network 202.101.90.0 0.0.0.255 area 10 R3(config-router)#network 192.168.12.0 0.0.0.255 area 10 R3(config-router)#network 60.154.101.0 0.0.0.255 area 10
R1	R1#configure terminal R1(config)#interface GigabitEthernet 0/0 R1(config-if-GigabitEthernet 0/0)#ip address 192.168.201.217 255.255.255.0 R1(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise 3 R1(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.201.1 R1(config-if-GigabitEthernet 0/0)#vrrp 2 priority 120 R1(config-if-GigabitEthernet 0/0)#vrrp 2 timers advertise 3 R1(config-if-GigabitEthernet 0/0)#vrrp 2 ip 192.168.201.2 R1(config-if-GigabitEthernet 0/0)#vrrp 2 track GigabitEthernet 2/1 30 R1(config-if-GigabitEthernet 0/0)#exit R1(config)#interface GigabitEthernet 2/1 R1(config-if-GigabitEthernet 2/1)#ip address 202.101.90.63 255.255.255.0 R1(config-if-GigabitEthernet 2/1)#exit R1(config)#router ospf R1(config-router)#network 202.101.90.0 0.0.0.255 area 10 R1(config-router)#network 192.168.201.0 0.0.0.255 area 10
R2	R2#configure terminal R2(config)#interface GigabitEthernet 0/0 R2(config-if-GigabitEthernet 0/0)#ip address 192.168.201.213 255.255.255.0 R2(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.201.1 R2(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise 3 R2(config-if-GigabitEthernet 0/0)#vrrp 1 priority 120 R2(config-if-GigabitEthernet 0/0)#vrrp 2 ip 192.168.201.2 R2(config-if-GigabitEthernet 0/0)#vrrp 2 timers advertise 3 R2(config-if-GigabitEthernet 0/0)#exit R2(config)#interface GigabitEthernet 1/1

	R2(config-if-GigabitEthernet 1/1)#ip address 60.154.101.3 255.255.255.0 R2(config-if-GigabitEthernet 1/1)#exit R2(config)#router ospf R2(config-router)#network 60.154.101.0 0.0.0.255 area 10 R2(config-router)#network 192.168.201.0 0.0.0.255 area 10
Verification	Run the **show vrrp** command to verify the configuration. ● Check whether R1, which acts as a master router in the group 2, reduces its VRRP group priority from 30 to 90 when it finds that the interface GigabitEthernet 2/1 connected to a WAN is unavailable. If yes, R2 in the group 2 becomes a master router. ● Check whether R1 increases its VRRP group priority from 30 to 120 when it finds the interface GigabitEthernet 2/1 connected to a WAN becomes available again. If yes, R1 becomes a master router again in the group 2.
R1	R1#show vrrp GigabitEthernet 0/0 - Group 1 State is Backup Virtual IP address is 192.168.201.1 configured Virtual MAC address is 0000.5e00.0101 Advertisement interval is 3 sec Preemption is enabled min delay is 0 sec Priority is 100 Master Router is 192.168.201.213 , priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.82 sec GigabitEthernet 0/0 - Group 2 State is Master Virtual IP address is 192.168.201.2 configured Virtual MAC address is 0000.5e00.0102 Advertisement interval is 3 sec Preemption is enabled min delay is 0 sec Priority is 120 Master Router is 192.168.201.217 (local), priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.59 sec

	Tracking state of 1 interface, 1 up: up GigabitEthernet 2/1 priority decrement=30
R2	R2#show vrrp GigabitEthernet 0/0 - Group 1 State is Master Virtual IP address is 192.168.201.1 configured Virtual MAC address is 0000.5e00.0101 Advertisement interval is 3 sec Preemption is enabled min delay is 0 sec Priority is 120 Master Router is 192.168.201.213 (local), priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.59 sec GigabitEthernet 0/0 - Group 2 State is Backup Virtual IP address is 192.168.201.2 configured Virtual MAC address is 0000.5e00.0102 Advertisement interval is 3 sec Preemption is enabled min delay is 0 sec Priority is 100 Master Router is 192.168.201.217 , priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.82 sec

1.4.2 Configuring VRRP-MSTP

Configuration Effect

- Link-level and gateway-level backup are achieved and network robustness is improved greatly when MTSP and VRRP are applied simultaneously.

Notes

- configure the routers in a VRRP backup group with the same virtual IPv4 address.
- Enabled VRRP on a Layer 3 interface.

Configuration Steps

Enabling IPv4 VRRP

- By default, IPv4 VRRP is not enabled on an interface. To enable IPv4 VRRP, please configure this item.

Configuring the IPv4 VRRP Authentication String

- By default, VRRP is in a non-authentication mode. To enable plain text password authentication for VRRP, please configure this item.

Configuring the IPv4 VRRP Advertisement Interval

- By default, a master router sends VRRP GWADV packets at an interface of one second. To manually set a value, please configure this item.

Configuring the IPv4 VRRP Preemption Mode

- By default, VRRP groups work in the preemption mode with zero-second delay.

Configuring the IPv4 VRRP Router Priority

- The default router priority for a VRRP group is 100. You can modify the priority based on your demand.

Configuring the IPv4 VRRP Tracked Interface

- By default, an IPv4 VRRP group monitors no interface. To achieve fault monitoring through monitoring an interface, please configure this item.

Configuring the IPv4 VRRP Learning Timer

- By default, timed learning is not enabled for a VRRP backup group. To enable backup routers to learn the VRRP GWADV packets from a master router, please configure this item.

Configuring the IPv4 VRRP Group Description

- By default, no description is configured for a VRRP group. To distinguish VRRP groups conveniently, please configure this item.

Configuring the IPv4 VRRP Delay

- By default, the VRRP delay for a VRRP group is not configured. Configure the delay to guarantee a stable transition from Non-preemption mode to Preemption mode.

Configuring the IPv4 VRRP Version

- By default, the VRRPv2 standard is adopted for IPv4 VRRP packets. To modify it manually, please configure this item.

Verification

- Run the **show vrrp** command to verify the configuration.

Related Commands

Enabling IPv4 VRRP

Command	**vrrp** *group* **ip** *ipaddress* [**secondary**]

Parameter Description	*group*: Indicates the VRID of a VRRP group, the range of which varies with product models. *Ipaddress*: The IP address of a VRRP group. **secondary**: Indicates the secondary IP address of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	If no virtual IP address is specified, routers cannot join a VRRP group. If no secondary IP address is applied, the configured IP address will be the primary IP address of a VRRP group.

Configuring the IPv4 VRRP Authentication String

Command	**vrrp** *group* **authentication** *string*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *string*: Indicates the authentication string of a VRRP group (a plain text password consists of 8 bytes at most).
Command Mode	Interface configuration mode
Usage Guide	In a VRRP group, the same authentication password should be configured for routers. The plain text authentication password cannot guarantee security but only prevents/prompts wrong VRRP configurations.

Configuring the IPv4 VRRP Advertisement Interval

Command	**vrrp** *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }
Parameter Description	*group*: Indicates the VRID of a VRRP group. *advertise-interval*: Indicates the advertisement interval of a VRRP group (unit: second). ***csec*** *centisecond-interval:* An interval for a master router in a backup group to send VRRP packets. It is an integer from 50 to 99. The unit is centisecond. No default value is provided. If it is configured for VRRPv2 packets, the default interval is one second.
Command Mode	Interface configuration mode
Usage Guide	If a router is elected as the Master in a VRRP group, it sends VRRP advertisement packets at the set interval to announce its VRRP state, priority and other information.

Configuring the IPv4 VRRP Preemption Mode

Command	**vrrp** *group* **preempt** [**delay** *seconds*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. **delay** *seconds*: Indicates the preemption delay for the Master router to claim its status. The default value is 0 second.
Command Mode	Interface configuration mode
Usage Guide	If a VRRP group runs in Preemption mode, a higher priority router will take the place of the lower priority Master. If a VRRP group runs in Non-preemption mode, a router with the priority higher than that of the Master remains Backup. It makes little sense to configure the Preemption mode when the VRRP group uses the IP address of an Ethernet interface, in which case the group has the highest priority and automatically becomes the Master in the group.

Configuring the IPv4 VRRP Router Priority

Command	**vrrp** *group* **priority** *level*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *level*: Indicates the priority of an interface in a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	This command is used to manually configure the priority of a VRRP group.

Configuring the IPv4 VRRP Tracked Interface

Command	**vrrp** *group* **track** *interface-type interface-number* [*priority*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. *interface-type interface-number*: Indicates the interface to be tracked. *priority*: Indicates the scale of VRRP priority change when the state of a monitored interface changes. The default value is 10.
Command Mode	Interface configuration mode
Usage Guide	A tracked interface must be a routable Layer-3 logic interface (for example, a Routed port, an SVI interface, and a Loopback interface). The priority of the router owns the virtual IP address associated with a VRRP group must be 255, and no tracked interface can be configured on it.

Configuring the IPv4 VRRP Tracked IP Address

Command	**vrrp** *group* **track** *ipv4-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. *ipv4-addres*: Indicates the IPv4 address to be tracked. **interval** *interval-value*: Indicates the probe interval. The unit is second. Unless configured manually, the value is 3 seconds by default. **timeout** *timeout-value*: Indicates the probe timeout of waiting for responses. If no response is received when the timeout is up, it is regarded that the destination is inaccessible. The unit is second. Unless configured manually, the value is 1 second by default. **retry** *retry-value*: Indicates the probe retries. If the probe packet is sent continually for retry-value times but no response is received, it is regarded that the destination is inaccessible. The unit is times. Unless configured, the value is 3 times by default. *priority*: Indicates the scale of VRRP priority change when the state of a monitored interface changes. The default value is 10.
Command Mode	Interface configuration mode
Usage Guide	To monitor a host, specify its IPv4 address for an IPv4 VRRP group. If a VRRP group owns the actual IP address of an Ethernet interface, the group priority is 255, and no monitored IP address can be configured.

Configuring the IPv4 VRRP Learning Timer

Command	**vrrp** *group* **timers learn**
Parameter	*group*: Indicates the VRID of a VRRP group.

Description	
Command Mode	Interface configuration mode
Usage Guide	Once the learning timer is enabled on a VRRP router, a Backup router learns the advertisement interval of the Master during the timer. Based on this, the Backup router calculates the interval for determining the Master router as failed instead of using the locally configured advertisement interval. This command achieves synchronization with the learning timer between the Master and Backup routers.

Configuring the IPv4 VRRP Group Description

Command	**vrrp** *group* **description** *text*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *text*: Indicates the description of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	A VRRP description helps distinguishing VRRP groups. A description has 80 bytes at most, otherwise wrong configuration is prompted.

Configuring the IPv4 VRRP Delay

Command	**vrrp delay** { **minimum** *min-seconds* | **reload** *reload-seconds* }
Parameter Description	**minimum** *min-seconds*: Indicates the VRRP delay after an interface state changes. **reload** *reload-seconds*: Indicates the VRRP delay after the system starts.
Command Mode	Interface configuration mode
Usage Guide	After the delay is configured for a VRRP group on an interface, the VRRP group starts after the delay instead of immediately upon system startup or the interface's resumption, ensuring non-preemption. If the interface receives a VRRP packet during the delay, the delay will be canceled and the VRRP will be started immediately. The two types of delay share a value range of 0 to 60 seconds.

Configuring the IPv4 VRRP Version

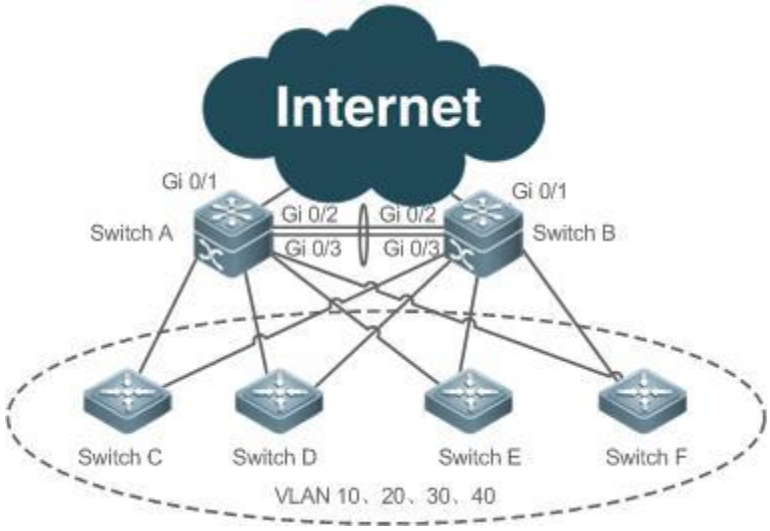
Command	**vrrp** *group* **version** { **2** | **3** }
Parameter Description	**2**: Indicates VRRPv2. **3**: Indicates VRRPv3.
Command Mode	Interface configuration mode
Usage Guide	Considering the compatibility between VRRPv2 and VRRPv3, specify a standard for IPv4 VRRP based on the actual network condition. VRRPv2 is developed in RFC3768, while VRRPv3 is described in RFC5798. This command is only applicable to IPv4 VRRP.

Configuration Example

Configuring VRRP+MSTP

Scenario

Figure 1- 8



Configuration Steps

- Enable MSTP on routers (switches A, B, C, D, E and F in this example). Configure VLAN-Instance mapping (mapping VLAN 10 and VLAN 20 to Instance 1, VLAN 30 and VLAN 40 to Instance 2, and the rest VLANs to Instance 0), and configure gateways (Switch A and Switch B in this example) as the root bridges of corresponding instances.
- Add the SVIs of all VLANs to corresponding VRRP backup groups, and configure gateways as the master and backup routers for corresponding backup groups See configuration details in the following table.

Gateway	VLAN ID	SVI	Backup Group	Virtual IP Address	State
Switch A	10	192.168.10.2	VRRP 10	192.168.10.1	Master
Switch B		192.168.10.3			Backup
Switch A	20	192.168.20.2	VRRP 20	192.168.20.1	Master
Switch B		192.168.20.3			Backup
Switch A	30	192.168.30.2	VRRP 30	192.168.30.1	Backup
Switch B		192.168.30.3			Master
Switch A	40	192.168.40.2	VRRP 40	192.168.40.1	Backup
Switch B		192.168.40.3			Master

- Configure the uplink port (port Gi 0/1 of Switch A and Switch B) of master routers as a monitored interface of master router.
- Step 1: Create VLAN. Create VLAN 10, VLAN 20, VLAN 30 and VLAN 40 respectively on Switch A and Switch B.
- Step 2: Configure MST regions. Map VLAN 10 and VLAN 20 to Instance 1, VLAN 30 and VLAN 40 to Instance 2, and the rest VLANs to Instance 0.
- Step 3: Configure Switch A as the root bridge for MST 0 and MST 1, and Switch B as the root bridge for MST 2.
- Step 4: Enable MSTP.
- Step 5: Configure SVIs of all the VLANs, add the SVIs to corresponding backup groups, and configure virtual IP addresses for the groups. See configuration in the above table.
- Step 6: Configure master routers and backup routers for all the groups.
- Step 7: Configure the uplink ports of master routers as monitored ports of VRRP groups. Caution: Monitored ports should be Layer 3 ports.

Step 8: Configure the Internet interfaces of the core routers as AP interfaces.

SwitchA	//Create VLAN 10, VLAN 20, VLAN 30 and VLAN 40 on Switch A.
	SwitchA#configure terminal
	Enter configuration commands, one per line. End with CNTL/Z.
	SwitchA(config)#vlan range 10,20,30,40
	SwitchA(config-vlan-range)#exit
	//Map VLAN 10 and VLAN 20 to Instance 1, VLAN 30 and VLAN 40 to Instance 2, and the rest VLANs to Instance 0.
	SwitchA(config)#spanning-tree mst configuration
	SwitchA(config-mst)#instance 1 vlan 10,20
	%Warning:you must create vlans before configuring instance-vlan relationship
	SwitchA(config-mst)#instance 2 vlan 30,40
	%Warning:you must create vlans before configuring instance-vlan relationship
	SwitchA(config-mst)#exit
	//On Switch A, configure the priority of MST 0 and MST 1 as 4096, and that of MST 2 as 8192.
	SwitchA(config)#spanning-tree mst 0 priority 4096
	SwitchA(config)#spanning-tree mst 1 priority 4096
	SwitchA(config)#spanning-tree mst 2 priority 8192
	//Enabling MSTP
	SwitchA(config)#spanning-tree
	Enable spanning-tree.
	//Configure SVIs of all the VLANs, add the SVIs to corresponding backup groups, and configure virtual IP addresses for the groups.
	SwitchA(config)#interface vlan 10
	SwitchA(config-if-VLAN 10)#ip address 192.168.10.2 255.255.255.0
	SwitchA(config-if-VLAN 10)#vrrp 10 ip 192.168.10.1
	SwitchA(config-if-VLAN 10)#exit
	SwitchA(config)#interface vlan 20
	SwitchA(config-if-VLAN 20)#ip address 192.168.20.2 255.255.255.0
	SwitchA(config-if-VLAN 20)#vrrp 20 ip 192.168.20.1
	SwitchA(config-if-VLAN 20)#exit
	SwitchA(config)#interface vlan 30
	SwitchA(config-if-VLAN 30)#ip address 192.168.30.2 255.255.255.0
	SwitchA(config-if-VLAN 30)#vrrp 30 ip 192.168.30.1
	SwitchA(config-if-VLAN 30)#exit

	SwitchA(config)#interface vlan 40
	SwitchA(config-if-VLAN 40)#ip address 192.168.40.2 255.255.255.0
	SwitchA(config-if-VLAN 40)#vrrp 40 ip 192.168.40.1
	SwitchA(config-if-VLAN 40)#exit
	//Increase the priority of the VRRP 10 and VRRP 20 of Switch A to 120.
	SwitchA(config)#interface vlan 10
	SwitchA(config-if-VLAN 10)#vrrp 10 priority 120
	SwitchA(config-if-VLAN 10)#exit
	SwitchA(config)#interface vlan 20
	SwitchA(config-if-VLAN 20)#vrrp 20 priority 120
	SwitchA(config-if-VLAN 20)#exit
	//Configure the Gi 0/1 port of Switch A as Route Port and its IP address as10.10.1.1/24.
	SwitchA(config)#interface gigabitEthernet 0/1
	SwitchA(config-if-GigabitEthernet 0/1)#no switchport
	SwitchA(config-if-GigabitEthernet 0/1)#ip address 10.10.1.1 255.255.255.0
	SwitchA(config-if-GigabitEthernet 0/1)#exit
	//Configure the Gi 0/1 port of Switch A as a monitored port for VRRP 10 and VRRP 20, and a *Priority decrement* of 30.
	SwitchA(config)#interface vlan 10
	SwitchA(config-if-VLAN 10)#vrrp 10 track gigabitEthernet 0/1 30
	SwitchA(config-if-VLAN 10)#exit
	SwitchA(config)#interface vlan 20
	SwitchA(config-if-VLAN 20)#vrrp 20 track gigabitEthernet 0/1 30
	SwitchA(config-if-VLAN 20)#exit
	//Configure ports Gi 0/2 and Gi 0/3 as AP ports, which are Trunk ports.
	SwitchA#configure terminal
	Enter configuration commands, one per line. End with CNTL/Z.
	SwitchA(config)#interface range gigabitEthernet 0/2-3
	SwitchA(config-if-range)#port-group 1
	SwitchA(config)#interface aggregateport 1
	SwitchA(config-if-AggregatePort 1)#switchport mode trunk

SwitchB	//Create VLAN 10, VLAN 20, VLAN 30 and VLAN 40 on Switch B. SwitchB#configure terminal Enter configuration commands, one per line. End with CNTL/Z. SwitchB(config)#vlan range 10,20,30,40

```
SwitchB(config-vlan-range)#exit
//Map VLAN 10 and VLAN 20 to Instance 1, VLAN 30 and VLAN 40 to Instance 2, and the rest VLANs to Instance 0.
SwitchB(config)#spanning-tree mst configuration
SwitchB(config-mst)#instance 1 vlan 10,20
%Warning:you must create vlans before configuring instance-vlan relationship
SwitchB(config-mst)#instance 2 vlan 30,40
%Warning:you must create vlans before configuring instance-vlan relationship
SwitchB(config-mst)#exit
//On Switch B, configure the priority of MST 2 as 4096, and that of MST 0 and MST 1 as 8192.
SwitchB(config)#spanning-tree mst 2 priority 4096
SwitchB(config)#spanning-tree mst 0 priority 8192
SwitchB(config)#spanning-tree mst 1 priority 8192
//Enabling MSTP
SwitchB(config)#spanning-tree
Enable spanning-tree.
//Configure SVIs of all the VLANs, add the SVIs to corresponding backup groups, and configure virtual IP addresses for the groups.
SwitchB(config)#interface vlan 10
SwitchB(config-if-VLAN 10)#ip address 192.168.10.3 255.255.255.0
SwitchB(config-if-VLAN 10)#vrrp 10 ip 192.168.10.1
SwitchB(config-if-VLAN 10)#exit
SwitchB(config)#interface vlan 20
SwitchB(config-if-VLAN 20)#ip address 192.168.20.3 255.255.255.0
SwitchB(config-if-VLAN 20)#vrrp 20 ip 192.168.20.1
SwitchB(config-if-VLAN 20)#exit
SwitchB(config)#interface vlan 30
SwitchB(config-if-VLAN 30)#ip address 192.168.30.3 255.255.255.0
SwitchB(config-if-VLAN 30)#vrrp 30 ip 192.168.30.1
SwitchB(config-if-VLAN 30)#exit
SwitchB(config)#interface vlan 40
SwitchB(config-if-VLAN 40)#ip address 192.168.40.3 255.255.255.0
SwitchB(config-if-VLAN 40)#vrrp 40 ip 192.168.40.1
SwitchB(config-if-VLAN 40)#exit
//Increase the priority of VRRP 30 and VRRP 40 of Switch B to 120.
```

	SwitchB(config)#interface vlan 30
	SwitchB(config-if-VLAN 30)#vrrp 30 priority 120
	SwitchB(config-if-VLAN 30)#exit
	SwitchB(config)#interface vlan 40
	SwitchB(config-if-VLAN 40)#vrrp 40 priority 120
	SwitchB(config-if-VLAN 40)#exit
	//Configure the Gi 0/1 port of Switch B as Route Port and its IP address as 10.10.1.1/24.
	SwitchB(config)#interface gigabitEthernet 0/1
	SwitchB(config-if-GigabitEthernet 0/1)#no switchport
	SwitchB(config-if-GigabitEthernet 0/1)#ip address 10.10.2.1 255.255.255.0
	SwitchB(config-if-GigabitEthernet 0/1)#exit
	//Configure the Gi 0/1 port of Switch B as a monitored port for VRRP 30 and VRRP 40, and the *Interface-Priority* as 30.
	SwitchB(config)#interface vlan 30
	SwitchB(config-if-VLAN 30)#vrrp 30 track gigabitEthernet 0/1 30
	SwitchB(config-if-VLAN 30)#exit
	SwitchB(config)#interface vlan 40
	SwitchB(config-if-VLAN 40)#vrrp 40 track gigabitEthernet 0/1 30
	SwitchB(config-if-VLAN 40)#exit
	//Configure ports Gi 0/2 and Gi 0/3 as AP ports, which are Trunk ports.
	SwitchB #configure terminal
	Enter configuration commands, one per line. End with CNTL/Z.
	SwitchB (config)#interface range gigabitEthernet 0/2-3
	SwitchB (config-if-range)#port-group 1
	SwitchB (config)#interface aggregateport 1
	SwitchB (config-if-AggregatePort 1)#switchport mode trunk

Verification	
Switch A	Check the configuration. SwitchA#show running-config ! vlan 10 ! vlan 20 ! vlan 30

```
!
vlan 40
!
spanning-tree
spanning-tree mst configuration
 instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
 instance 1 vlan 10, 20
 instance 2 vlan 30, 40
spanning-tree mst 0 priority 4096
spanning-tree mst 1 priority 4096
spanning-tree mst 2 priority 8192
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.10.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 port-group 1
!
interface GigabitEthernet 0/3
 port-group 1
!
interface AggregatePort 1
 switchport mode trunk
!
interface VLAN 10
 no ip proxy-arp
 ip address 192.168.10.2 255.255.255.0
 vrrp 10 priority 120
 vrrp 10 ip 192.168.10.1
 vrrp 10 track GigabitEthernet 0/1 30
!
interface VLAN 20
 no ip proxy-arp
```

```
  ip address 192.168.20.2 255.255.255.0
  vrrp 20 priority 120
  vrrp 20 ip 192.168.20.1
  vrrp 20 track GigabitEthernet 0/1 30
!
interface VLAN 30
  no ip proxy-arp
  ip address 192.168.30.2 255.255.255.0
  vrrp 30 ip 192.168.30.1
!
interface VLAN 40
  no ip proxy-arp
  ip address 192.168.40.2 255.255.255.0
  vrrp 40 ip 192.168.40.1
//Check VRRP status.
SwitchA#show vrrp brief
Interface    Grp    Pri    timer    Own    Pre    State      Master addr      Group addr
VLAN 10      10     120    3        -      P      Master     192.168.10.2     192.168.10.1
VLAN 20      20     120    3        -      P      Master     192.168.20.2     192.168.20.1
VLAN 30      30     100    3        -      P      Backup     192.168.30.3     192.168.30.1
VLAN 40      40     100    3        -      P      Backup     192.168.40.3     192.168.40.1
//Disconnect the uplink of Switch A, and check VRRP status.
SwitchA#show vrrp brief
Interface    Grp    Pri    timer    Own    Pre    State      Master addr      Group addr
VLAN 10      10     90     3        -      P      Backup     192.168.10.3     192.168.10.1
VLAN 20      20     90     3        -      P      Backup     192.168.20.3     192.168.20.1
VLAN 30      30     100    3        -      P      Backup     192.168.30.3     192.168.30.1
VLAN 40      40     100    3        -      P      Backup     192.168.40.3     192.168.40.1
```

Switch B

```
//Check the configuration.
SwitchB#show running-config
!
vlan 10
```

```
!
vlan 20
!
vlan 30
!
vlan 40
!
spanning-tree
spanning-tree mst configuration
  instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
  instance 1 vlan 10, 20
  instance 2 vlan 30, 40
spanning-tree mst 0 priority 8192
spanning-tree mst 1 priority 8192
spanning-tree mst 2 priority 4096
interface GigabitEthernet 0/1
  no switchport
  no ip proxy-arp
  ip address 10.10.2.1 255.255.255.0
!
interface GigabitEthernet 0/2
  port-group 1!
interface GigabitEthernet 0/3
  port-group 1
!
interface AggregatePort 1
  switchport mode trunk
!
interface VLAN 10
  no ip proxy-arp
  ip address 192.168.10.3 255.255.255.0
  vrrp 10 ip 192.168.10.1
!
interface VLAN 20
```

```
 no ip proxy-arp
 ip address 192.168.20.3 255.255.255.0
 vrrp 20 ip 192.168.20.1
!
interface VLAN 30
 no ip proxy-arp
 ip address 192.168.30.3 255.255.255.0
 vrrp 30 priority 120
 vrrp 30 ip 192.168.30.1
 vrrp 30 track GigabitEthernet 0/1 30
!
interface VLAN 40
 no ip proxy-arp
 ip address 192.168.40.3 255.255.255.0
 vrrp 40 priority 120
 vrrp 40 ip 192.168.40.1
 vrrp 40 track GigabitEthernet 0/1 30
//Check VRRP status.
SwitchB#show vrrp brief
Interface    Grp    Pri    timer    Own    Pre    State      Master addr      Group addr
VLAN 10      10     100    3        -      P      Backup     192.168.10.2     192.168.10.1
VLAN 20      20     100    3        -      P      Backup     192.168.20.2     192.168.20.1
VLAN 30      30     120    3        -      P      Master     192.168.30.3     192.168.30.1
VLAN 40      40     120    3        -      P      Master     192.168.40.3     192.168.40.1
//Disconnect the uplink of Switch B, and check VRRP status.
SwitchB#show vrrp brief
Interface    Grp    Pri    timer    Own    Pre    State      Master addr      Group addr
VLAN 10      10     100    3        -      P      Master     192.168.10.3     192.168.10.1
VLAN 20      20     100    3        -      P      Master     192.168.20.3     192.168.20.1
VLAN 30      30     120    3        -      P      Master     192.168.30.3     192.168.30.1
VLAN 40      40     120    3        -      P      Master     192.168.40.3     192.168.40.1
```

1.5 Monitoring

Displaying

Description	Command
Displays the brief or detailed information about IPv4 VRRP.	**show vrrp** [**brief** | *group*]
Displays the information about an IPv4 VRRP group on a specified interface.	**show vrrp interface** *type number* [**brief**]
Displays the statistics of VRRP packets.	**show vrrp packet statistics** [*interface-type interface-number*]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs VRRP errors, events, packets and status.	**debug vrrp**
Debugs VRRP errors.	**debug vrrp errors**
Debugs VRRP events.	**debug vrrp events**
Debugs VRRP packets.	**debug vrrp packets** [**acl** *acl-id* | [**icmp** | **protocol**] **interface** *type number* [*group*]]
Debugs VRRP status.	**debug vrrp state**

2 Configuring RNS

2.1 Overview

The reliable network service (RNS) tests specific services provided by a peer device to monitor the service availability, integrity of the end-to-end connection, and service quality. Using the RNS test results, you can:

- Learn the network performance in time and take measures accordingly to handle related network performance problems.
- Diagnose and locate network faults.

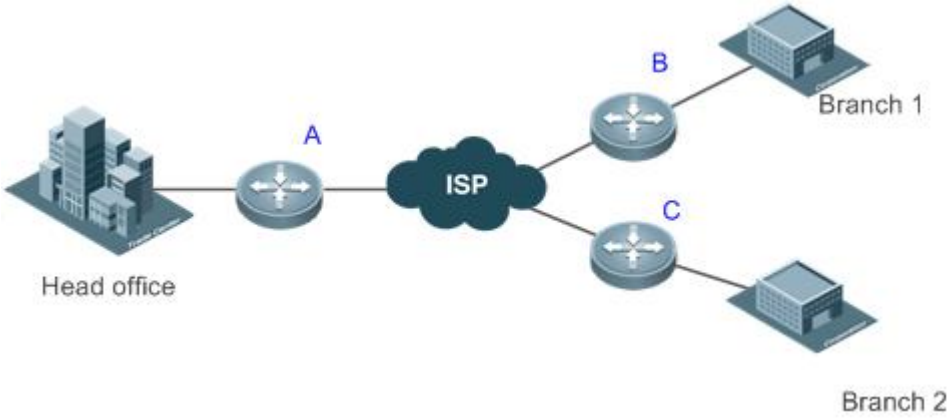
2.2 Applications

2.2.1 Testing and Evaluating Service Performance

Scenario

As shown in the following figure, a company is going to deploy a video conference system between the headquarters and branches, and has completed the related quality of service (QoS) configurations. Before formal deployment, it must be checked whether the services can be provisioned normally under the existing service pressure of the company. The video conference system is sensitive to the User Datagram Protocol (UDP) delay and UDP transmission jitter of the network. The traditional ping tool can test the Internet Control Message Protocol (ICMP) performance, but cannot effectively evaluate the UDP transmission performance and cannot meet the requirement for jitter measurement.

Figure 2-1



Remarks	A, B, and C are switches.

Deployment

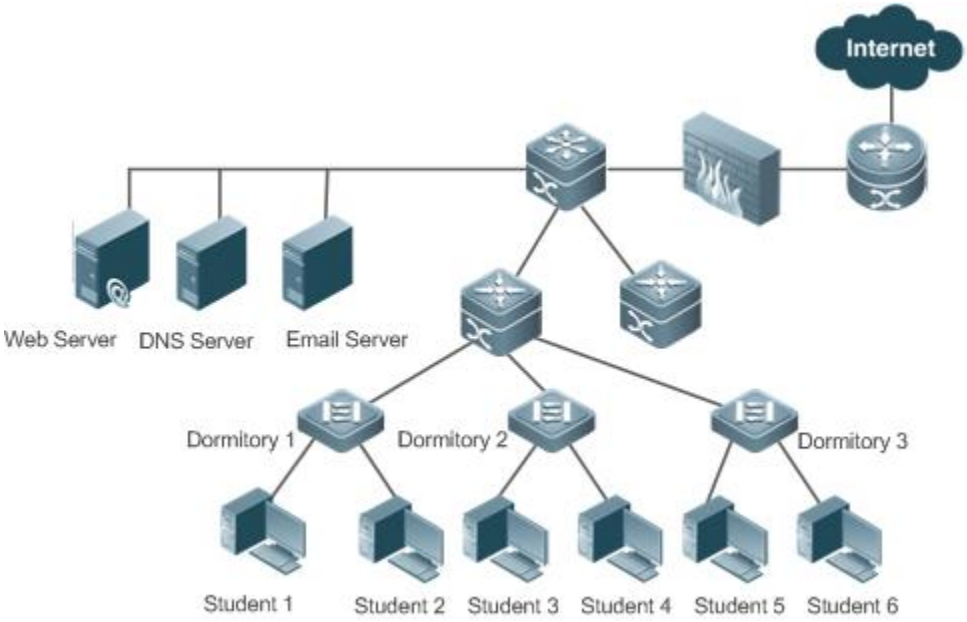
- Configure RNS on the egress switching device or switch of each branch to test the UDP jitter and delay.
- On Switch A, specify the IP address and UDP port of the egress switching device or switch in the headquarters, and then UDP packets can be automatically sent. Based on the configurations, the egress switching device or switch in the headquarters can automatically respond to the UDP packets. The egress switching device or switch of the branch processes the sent and received packets, and calculates the UDP jitter. To learn the performance in different periods of time, you also need to configure scheduling functions, such as periodically start/stop and repeated running, for the RNS.

2.2.2 Locating Network Faults

Scenario

On the campus network as shown in Figure 2-2, Student 1 reports a Web server access failure, Student 3 reports an Internet access failure, and Student 6 reports an email sending/receiving failure.

Figure 2-2



Deployment

- The administrator directly enables the DNS function on the access switch of the dormitories to test whether the domain name service (DNS) server is faulty. If DNS fails, an ICMP echo packet is automatically triggered to test whether the Web server is reachable.
- When a fault occurs, the administrator only needs to start a test, and the subsequent tests can be automatically triggered. Then, the administrator can check the test results to locate the fault, which greatly reduces the workload for the administrator.

2.3 Features

Basic Concepts

↘ RNS Instance

An RNS instance can be treated as an RNS process. Before performing the RNS, you must create an RNS instance. In the RNS instance, you need to configure the RNS parameters, such as the test type, test destination address, and test frequency. The instance ID is globally unique.

Feature	Description
RNS Instance	Monitor the network connectivity, service availability, integrity of end-to-end connection, and service quality.
Track Support for the RNS	Track the test results and notify the related module of the results.

2.3.1 RNS Test

Monitor the network connectivity, service availability, integrity of end-to-end connection, and service quality. For example, test whether the DNS function of the device is normal. Currently, the RNS supports the following types of tests: ICMP echo, and DNS.

Working Principle

ICMP Echo Test

ICMP echo is a basic function of the RNS, and is implemented in compliance with the RFC 2925. An ICMP packet is sent to check whether the destination is reachable and to calculate the network response time and packet loss rate.

An ICMP echo request packet is sent to the destination IP address based on the preset test time and frequency. Upon receipt of the ICMP echo request packet, an ICMP echo reply packet is returned from the destination IP address. Through the ICMP echo test, the response time and packet loss rate is calculated based on the information relating to the received ICMP echo reply packet, for example, the receipt time and number of packets. In this way, the current network performance and status are reflected. The ICMP echo test results and historical records will be recorded, and you can use the command line to display them.

The prerequisite for a successful ICMP echo test is that destination devices can correctly respond to ICMP echo request packets.

DNS Test

In a DNS test, a DNS client is simulated to send a domain name resolution request to a specified DNS server. You can determine whether the DNS server is available and the domain name resolution speed by checking the domain name resolution result and the time required for domain name resolution. In the DNS test, the domain name resolution process is simulated, and the mapping between the resolved domain name and the IP address is not saved. The DNS test results and historical records will be recorded in the test group. You can use the command line to check the test results and historical records.

Procedure for Configuring an RNS Instance Test

8. Create an instance and configure the test based on the test type.
9. Start the instance.
10. Use the RNS instance to construct a packet of the specific test type and send the packet to the peer end.
11. Upon receipt of the test packet, the peer end returns a reply packet of a corresponding type.
12. The RNS instance calculates the packet loss rate and round trip time based on whether a reply packet is received and the time of reply packet receipt.
13. Use the show or debug command to check the test result.

The preceding describes general procedures for RNS instance tests. For details about configuration, see the following sections.

Related Configuration

Configuring the Test Repeat Interval

By default, the test repeat interval is 60s.

In RNS configuration mode, run the **frequency** *millisecond* command to configure the test repeat interval.

Configure the frequency based on the following formula to ensure correct test calculation.

(**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *milliseconds*)

Configuring the Test Timeout

The default timeout varies according to the test type. You can run the **show ip rns configuration** command to display the timeout of a specific test type.

In RNS configuration mode, run the **timeout** *milliseconds* command to configure the timeout of an instance.

Configure the timeout based on a formula. For details, see the "Usage Guide" of the **frequency** command.

Configure the test time threshold.

Configuring the Test Threshold

By default, the test threshold is 5,000 ms.

In RNS configuration mode, run the **threshold** *milliseconds* command to configure the instance test threshold.

Configure the threshold based on a formula. For details, see the "Usage Guide" of the **frequency** command.

Configuring a Tag for the Test

No default configuration is available.

In RNS configuration mode, run the **tag** *text* command to configure a test tag.

You can run the **tag** command to specify a tag to identify the test.

Configuring the Protocol Payload Size

The default protocol payload size varies with the test type. By default, the protocol payload size is the minimum or appropriate size for protocol packets of the corresponding test type.

In RNS configuration mode, run the **request-data-size** *bytes* command to configure the protocol payload size.

Perform this configuration in IP RNS configuration mode.

Configuring the TOS Field of the Test Packet

By default, the TOS is 0.

In RNS configuration mode, run the **tos** number command to configure the TOS field in the IPv4 header of RNS test packets.

2.3.2 Track Support for the RNS

Objects that can be tracked include: test result of an RNS instance, RNS list status, link status on an interface, and track list status. When the track status changes, an action of other modules is triggered.

Working Principle

The test result of an RNS instance is tracked as follows:

- Configure a track object for tracking the test result of an RNS instance.
- When the test result of the RNS instance changes, the RNS module sends a status change message to the track module.
- The track module receives the test result. After the preset delay, if the test result remains unchanged, the status of the track object is modified, and the module of the track object is notified of the modification. If the test result recovers within the period, the status of the track object is not modified and the corresponding module is not notified.

Related Configuration

Configuring a Track Object for Tracking the Link Status of An Interface

By default, the function of tracking the link status of an interface is disabled.

Run the **track interface line-protocol** command to configure a track object, which is used to track the link status of an interface.

If the link status of the interface is UP, the status of the track object is UP. If the link status of the interface is DOWN, the status of the track object is also DOWN.

Configuring a Track Object for Tracking the Test Result of an RNS Instance

By default, the function of tracking the test result of an RNS instance is disabled.

Run the **track rns** command to configure a track object, which is used to track the test result of an RNS instance. The RNS instance ID ranges from 1 to 500.

If the RNS test succeeded, the track object is in Up state. If the RNS test failed, the track object is in Down state.

Configuring a Track Object for Tracking the Status of a Track List

By default, the function of tracking the status of a track list is disabled.

Run the **track list** command to configure a track object, which is used to track the status of a track list. The result can be the AND or OR operation result of all member status.

If the result of this track object is set to the OR operation result of all member status, when all RNS tests succeeded, the track object is in Up state. If one RNS test failed, the track object is in Down state. If the result of this track object is set to the OR operation result of all member status, when all RNS tests failed, the track object is in Down state. If one RNS test succeeded, the track object is in Up state.

Configuring a Track List Member

By default, no member is configured for the track list.

Run the **object** command to configure a track list member. The status of the member can be the same as or contrary to that of the corresponding track object.

Adjusting the Delay for Notifying the Status Change of a Track Object

By default, the delay for notifying the status change of a track object is 0.

Run the **delay** command to adjust the delay for track notification, including the delay for notifying the status change of a track object from UP to DOWN and the delay for notifying the status change of a track object from DOWN to UP. The delay ranges from 0 to 180. The unit is second.

A longer delay indicates that it takes more time before the module that is concerned with the track object is notified of the status. A shorter delay indicates that it takes less time before the module that is concerned with the track object is notified of the status.

2.4 Configuration

Configuration Item	Description and Command
Configuring RNS Basic Functions	(Mandatory) It is used to configure basic function parameters of the RNS.

Configuration Item	Description and Command	
	ip rns	Supports detailed configuration and brief configuration. ● Detailed configuration: An RNS operation object is defined, and used as the configuration ID for subsequent tests and parameters. ● Brief configuration: Subsequent configuration is not required, and tests can be started in one step. Currently, ICMP echo, DNS, can be started in one step.
	ip rns reaction-configuration	Configures the proactive threshold monitoring and triggering mechanism of the RNS test.
	ip rns reaction-trigger	Triggers another type of the RNS test in pending state when the monitoring threshold exceeds the expectation during an RNS test.
	ip rns schedule	Configures the scheduling method, start time, and life time of an RNS test.
	ip rns restart	Restarts an RNS test.
	ip rns reset	Clears all the IP RNS configurations.
Configuring the ICMP Echo Test	(Optional) It is used to implement the ICMP echo test.	
	icmp-echo	Creates an ICMP echo test instance.
	request-data-size	Configures the protocol payload size.
	frequency	Configures the test repeat interval.
	tag	Configures a tag.
	threshold	Configures the test time threshold.
	timeout	Configures the test timeout.
	tos	Configures the TOS field in the IPv4 header of test packets.
Configuring the DNS Test	(Optional) It is used to implement the DNS test.	
	dns	Creates a DNS test instance.
	frequency	Configures the test repeat interval.
	tag	Configures a tag.
	threshold	Configures the test time threshold.
	timeout	Configures the test timeout.
	tos	Configures the TOS field in the IPv4 header of test packets.
Configuring the Track Support for the RNS	(Optional) It is used to configure the track support for other test modules.	
	track rns	Configures a track object for tracking the test result of an RNS instance.
	track interface line-protocol	Configures a track object for tracking the link status of an interface.
	track list	Configures a track object for tracking the status of a track list.
	object	Configures a member object for a track list object.
	delay	Configures the delay for notifying the status change of a track object.

2.4.1 Configuring RNS Basic Functions

Configuration Effect

- Detailed configuration: Configures an RNS instance to complete basic configuration of the RNS instance.
- Brief configuration: Configure and start an RNS instance at a time. (Optional)

Notes

- In detailed configuration mode, if you do not configure the test type after entering the IP RNS mode by running the command, the RNS instance will not be created.
- In detailed configuration mode, after configuring an RNS instance, you need to run the **ip rns schedule** command to configure the startup policy; otherwise, the test will not be implemented.

Configuration Steps

Defining an RNS Operation Object

- Mandatory.
- Unless otherwise required, define an RNS operation object on each switch.
- Brief configuration is optional.

Configuring the Proactive Threshold Monitoring and Triggering Mechanism for an RNS Test

- Perform this configuration if it is required to configure the proactive threshold monitoring and triggering mechanism for the test.
- Perform this configuration on every switching device unless otherwise required.

Enabling an RNS Instance to Trigger Another RNS Instance

- Perform this configuration if it is required to trigger another RNS test in pending state when the monitoring threshold exceeds the expectation during an RNS test.
- If schedule parameters are not configured for the triggered RNS instance, the default schedule parameters are applied.
- Unless otherwise required, apply this configuration to each switch.

Configuring Schedule Parameters of an RNS Instance

- Perform this configuration on every switching device unless otherwise required.
- In the case of brief configuration, this command is already configured using the default values, and manual configuration is not required.

Restarting an RNS Instance

- Perform this configuration, or directly run the **ip rns schedule X start-time now** command if it is required to restart an IP RNS instance in pending state.

Clearing Configurations of All RNS Instances

- Perform this configuration if it is required to clear configurations of all the IP RNS instances, for example, when a lot of instances are configured but configurations are found incorrect.

Verification

- Run the **show ip rns configuration** command to display configurations of RNS instances.

Related Commands

Defining an IP RNS Operation Object

Command	**ip rns** *operation-number*
Parameter Description	*operation-number*: Indicates the RNS instance ID. The value ranges from 1 to 500.
Command Mode	Global configuration mode
Usage Guide	Currently, the RNS supports only IPv4-related tests,. At most 500 tests can be configured, depending on the performance of devices. The test function is only a value-added function. When a large number of tests are configured and consume a lot of system resources, the test function may be temporary disabled to ensure normal operation of core services, such as route forwarding. Detailed configuration (executing mandatory items of **ip rns** *operation-number*): Run this command and enter the IP-RNS configuration mode. In this mode, you can define various test types. If the test type is not configured, the RNS test is not created. After configuring an RNS test, you must run the **ip rns schedule** command to configure its schedule parameters; otherwise, the test cannot be conducted. After configuring the type of an RNS test, you can run the **ip rns** command to enter the mode of the test type. To modify the type of an RNS instance, you need to first delete the RNS instance by running the **no ip rns** command in global configuration mode.

Configuring the Proactive Threshold Monitoring and Triggering Mechanism for the Test

Command	**ip rns reaction-configuration** *operation-number* **react** *monitored-element*[**action-type** *option*][**threshold-type** {**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate**|**never**| **xofy**[*x-value y-value*] }] [**threshold-value** *upper-threshold lower-threshold*]
Parameter Description	*operation-number*: Indicates the RNS instance ID. The value ranges from 1 to 500. *monitored-element*: Specifies the monitored element. **action-type** *option*: Indicates the action taken after the test is triggered. **average** [*number-of-measurements*]: Indicates that the subsequent associated actions are triggered if the average of *number-of-measurements* of the monitored element exceeds the threshold. **consecutive** [*occurrences*]: Indicates that the test is triggered if the consecutive number of *occurrences* of the monitored element exceeds the threshold. The default value of *occurrences* is 5. The value ranges from 1 to 16. **immediate**: Indicates that the test is triggered immediately after the monitored element exceeds the threshold. **never**: Indicates that the test is never triggered. **xofy** [*x-value y-value*]: Indicates that results of X tests exceed the threshold in the last Y tests. The default values of X and Y are 5. The value of X or Y ranges from 1 to 16. **threshold-value** *upper-threshold lower-threshold*: Indicate the upper and lower thresholds. ● When ***monitored-element*** *is* **rtt**, the thresholds are the time. For default values, see "Usage Guide". The value ranges from 0 to 60,000 ms. ● Note that you do not need to configure **threshold-value** when **react** is set to **timeout**.

Command Mode	Global configuration mode
Usage Guide	You can configure multiple thresholds for one RNS test to monitor different elements. The following table provides the mapping between test types and monitored elements.

monitored-element	icmp-echo	dns
timeout		
rtt		

The following table lists the default thresholds of each monitored element.

Monitored Element	Upper Threshold	Lower Threshold
timeout	-	-
rtt	5000ms	0ms

Enabling an RNS Instance to Trigger Another RNS Instance

Command	**ip rns reaction-trigger** *operation-number target-operation*
Parameter Description	*operation-number*: Indicates the number of the source RNS instance that triggers the action. The value ranges from 1 to 500. *target-operation*: Indicates the number of the target RNS instance that is triggered. The value ranges from 1 to 500.
Command Mode	Global configuration mode
Usage Guide	The trigger function is generally used in network fault diagnosis scenario. In a common scenario, you do not need to configure the trigger function.

Configuring Schedule Parameters of an RNS Instance

Command	**ip rns schedule** *operation-number*[**life**{ **forever**|*seconds*}] [**start-time**{ *hh:mm*[*:ss*] [*month day*|*daymonth*] |**pending**|**now**|**after***hh:mm:ss}*] [**recurring**]
Parameter Description	*operation-number*: Indicates the number of the RNS operation. The value ranges from 1 to 500. **lifeforever**: Indicates that the RNS operation life time is valid forever. **life** *seconds*: Indicates the running time of the RNS instance in seconds. *hh:mm[:ss]*: Indicates the start time of the RNS instance, in 24-hour format. *month*: Indicates the start month of the RNS instance. The default value is the current month. *day*: Indicates the start date of the RNS instance. The default value is the current date. **pending**: Indicates that the start time of the RNS instance is not defined, which is the default. **now**: Indicates that the operation start time is now, that is, the operation starts now. **after***hh:mm:ss*: Indicates that the RNS instance starts after a delay of hh:mm:ss. **recurring**: Indicates whether the RNS instance starts at the same time every day.
Command	Global configuration mode

Mode	
Usage Guide	If the schedule parameters of an RNS instance have been configured by running the **ip rns schedule** command, parameters cannot be modified during running. To modify the configuration, you need to run the **no ip rns schedule** command to delete the schedule parameters. life { *seconds* } indicates the running time of the RNS instance. That is, the test stops after a period of time in seconds.

Restarting an RNS Test by Running the ip rns restart Command

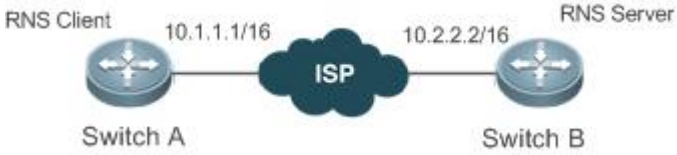
Command	**ip rns restart** *operation-number*
Parameter Description	*operation-number*: Indicates the number of the RNS instance. The value ranges from 1 to 500.
Command Mode	Global configuration mode
Usage Guide	This command restarts an RNS test for which the scheduling policy is configured and is in pending state. This command is invalid for an RNS test for which the scheduling policy is not configured.

Clearing Configurations of All the IP RNS Instances by Running the ip rns reset Command

Command	**ip rns reset**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This command clears configurations of all the IP RNS instances. It is used only in extreme cases, for example, when a lot of RNS tests are configured but the configurations are found incorrect.

Configuration Example

Configuring RNS Basic Functions

Scenario **Figure 2- 3**	
Configuration Steps	● Configure instance 1 on Switch A. ● Configure the scheduling method, start time, and life time of instance 1. ● Configure the proactive threshold monitoring and triggering mechanism of instance 1. ● Trigger instance 2 in pending state when the monitoring threshold of instance 1 exceeds the expectation.
Switch A	A# configure terminal A(config)# ip rns 1 A(config-ip-rns)#icmp-echo 10.1.1.1

	A(config-ip-rns-icmp-echo)#exit A(config)ip rns schedule 1 start-time now life forever A(config)ip rns reaction-configuration 1 react timeout threshold-type immediate action-type trigger A(config)ip rns reaction-trigger 1 2
Verification	Run the **show ip rns configuration** command to display the instance configurations. Router#show ip rns configuration 1 Entry number: 1 Tag: fs555 Type of operation to perform: icmp-echo Operation timeout (milliseconds): 5000 Operation frequency (milliseconds): 60000 Threshold (milliseconds): 5000 Recurring (Starting Everyday): FALSE Life (seconds): 3500 Next Scheduled Start Time:Start Time already passed Target address/Source address: 2.2.2.3/0.0.0.0 Request size (ARR data portion): 36

2.4.2 Configuring the ICMP Echo Test

Configuration Effect

Create an ICMP echo test instance.

Notes

- The RNS basic functions must be configured.

Configuration Steps

Creating an ICMP Echo Test Instance

- Mandatory.
- Unless otherwise required, create ICMP echo test instances on each switch.

Configuring Common Optional Parameters of the Test

- Mandatory if common optional parameters of the test, for example, the repeat interval, tag, time threshold, timeout, and TOS, are required to be changed..
- Perform this configuration on every switching device unless otherwise required.

Configuring the Protocol Payload Size

- Perform this configuration if it is required to change the protocol payload size of the test.
- Perform this configuration on every switching device unless otherwise required.

Verification

- Run the **show ip rns configuration** command to display the instance configurations.

Related Commands

Creating an ICMP Echo Test Instance

Command	**icmp-echo** { **oob** { *destination-ip-address* | *destination-hostname* [**name-server** *ip-address*] } [**source-ipaddr** *ip-address*] **via** *type num* **next-hop** *ip-address* } | { { *destination-ip-address* | *destination-hostname* [**name-server** *ip-address*] } [**source-ipaddr** *ip-address*] [**af-direct**] **out-interface** *type num* [**next-hop** *ip-address*]] }
Parameter Description	**oob**: Indicates the test on the MGMT interface. *destination-ip-address*: Indicates the destination IP address. *destination-hostname*: Indicates the destination host name. **name-server** *ip-address*: Specifies the DNS server when the destination host name is configured. By default, the DNS server configured by using the **ipname-server** command is used for address resolution. **source-ipaddr** *ip-address*: Indicates the source IP address. **out-interface** *type num*: Specifies the outgoing interface (non-MGMT interface) of the test packet. **af-direct**: Allows packets to be sent and received without the protocol stack during the RNS test. **via** *type num*: Specifies the MGMT interface as the outgoing interface of the test packet. **next-hop** *A.B.C.D*: Indicates the IP address of the next hop.
Command Mode	IP RNS configuration mode (config-ip-rns)
Usage Guide	After an ICMP echo test is started, the system sends an ICMP echo request packet to test whether the device is connected to the target host. After an ICMP-Echo test instance is created, the system enters the IP RNS ICMP echo mode. By default, the protocol payload size of an ICMP echo request packet is 36 bytes. You can run the **request-data-size** command to change the packet size. You need to configure the RNS test type (for example, ICMP echo and DNS) before configuring parameters. To modify the type of an RNS instance, you need to delete the RNS instance by running the **no ip rns** command in global configuration mode.

Configuring the Protocol Payload Size of an RNS Instance

Command	**request-data-size** *bytes*
Parameter Description	*bytes*: Indicates the bytes of a test packet. The minimum and maximum bytes vary with the test type. You need to configure this parameter based on the command prompt in corresponding test mode.
Command Mode	IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo)
Usage Guide	This command is used to stuff some bytes in the test packet so that large packets can be used for the test.

Configuring the Test Repeat Interval

Command	**frequency** *milliseconds*
Parameter Description	*milliseconds*: Indicates the packet sending interval in ms. The default value is 60,000 ms. The value ranges from 10 to 604,800,000. The maximum value is one week.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo)
Usage Guide	After an RNS instance is started, tests are conducted periodically. You can run the **frequency** command to specify the repeat interval. You need to configure the frequency based on the following formula to ensure correct test calculation. (**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *milliseconds*)

Configuring a Tag for an RNS Instance

Command	**tag** *text*
Parameter Description	*text*: Sets the test tag. The value is a string of up to 79 characters.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo)
Usage Guide	This command specifies a tag for a test, which is often used to indicate the function of the test.

Configuring the Time Threshold for an RNS Instance

Command	**threshold** *milliseconds*
Parameter Description	*milliseconds*: Indicates the time threshold for the test. The value ranges from 0 to 60,000, in the unit of milliseconds. The default value is 5,000.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo)
Usage Guide	Configure the threshold based on the following formula to ensure correct test calculation. (**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *milliseconds*)

Configuring the Timeout for an RNS Instance

Command	**timeout** *millisecond*
Parameter Description	*millisecond*: Indicates the test timeout. The value ranges from 10 to 604,800,000. The unit is ms. The default timeout varies according to the test type.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo)
Usage Guide	Configure the timeout based on the following formula to ensure correct test calculation. (**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *milliseconds*)

Configuring the TOS Field in the IPv4 Packet Header of an IP RNS Test

Command	**tos** *number*
Parameter Description	*number*: Sets the TOS field in the IPv4 header of test packets. The value ranges from 0 to 255. The default value is 0.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo)
Usage Guide	TOS is a 8-bit field in the IPv4 packet header. By setting the TOS, you can control the priority of the test packet. For different TOS fields, the processing priorities are different on the intermediate routers.

Configuration Example

Figure 2- 4	
	Configure RNS instance 1 and related parameters on Switch A.
Switch A	A# configure terminal A(config)# ip rns 1 A(config-ip-rns)#icmp-echo 10.2.2.2 A(config-ip-rns-icmp-echo)#exit A(config)#ip rns schedule 1 start-time now life forever
	Run the **show ip rns configuration** command to display the instance configurations.
Switch A	A#show ip rns configuration 1 Entry number: 1 Tag: Type of operation to perform: icmp-echo Operation timeout (milliseconds): 5000 Operation frequency (milliseconds): 60000 Threshold (milliseconds): 5000 Recurring (Starting Everyday): FALSE Life (seconds): foerver Next Scheduled Start Time:Start Time already passed Target address/Source address: 10.2.2.2/0.0.0.0 Request size (ARR data portion): 36

2.4.3 Configuring the DNS Test

Configuration Effect

Create a DNS test instance.

Notes

- The RNS basic functions must be configured.

Configuration Steps

Creating a DNS Test Instance

- Mandatory.
- Unless otherwise required, create DNS test instances on each switch.

Configuring Common Optional Parameters of the Test

- Mandatory if common optional parameters of the test, for example, the repeat interval, tag, time threshold, timeout, and TOS, are required to be changed.
- Perform this configuration on every switching device unless otherwise required.

Verification

- Run the **show ip rns configuration** command to display the instance configurations.

Related Commands

Creating a DNS Test Instance

Command	**dns** { **oob** *destination-hostna*me **name-server** *ip-address* [**source-ipaddr** *ip-address*] **via** *type num* **next-hop** *ip-address* } | { *destination-hostname* **name-server** *ip-address* [**source-ipaddr** *ip-address*] [**[af-direct]** **out-interface** *type num* [**next-hop** *ip-address*]] }
Parameter Description	**oob**: Indicates the test on the MGMT interface. *destination-hostname*: Indicates the destination host name. **name-server** *ip-address*: Indicates the DNS IP address. **source-ipaddr** *ip-address:* Indicates the source IP address. **out-interface type** *num*: Specifies the outgoing interface (non-MGMT interface) of the test packet. **af-direct**: Allows packets to be sent and received without the protocol stack during the RNS test. **via** *type num*: Specifies the MGMT interface as the outgoing interface of the test packet. **next-hop** *ip-address*: Indicates the IP address of the next hop when the outgoing interface is specified.
Command Mode	IP RNS configuration mode (config-ip-rns)
Usage Guide	After a DNS test is started, the system sends a DNS parsing request packet to test whether the device is connected to the target host. After a DNS test instance is created, the system enters the IP RNS DNS mode. You need to configure the RNS test type before configuring parameters. To modify the type of an RNS instance, you need to delete the RNS instance by running the **no ip rns** command in global configuration mode.

Configuring the Test Repeat Interval

Command	**frequency** *milliseconds*
Parameter Description	*milliseconds*: Indicates the packet sending interval in ms. The default value is 60,000 ms. The value ranges from 10 to 604,800,000. The maximum value is one week.
Command	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo)

Mode	
Usage Guide	After an RNS instance is started, tests are conducted periodically. You can run the **frequency** command to specify the repeat interval. You need to configure the frequency based on the following formula to ensure correct test calculation. (**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *milliseconds*)

Configuring a Tag for an RNS Instance

Command	**tag** *text*
Parameter Description	*text*: Sets the test tag. The value is a string of up to 79 characters.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo)
Usage Guide	This command specifies a tag for a test, which is often used to indicate the function of the test.

Configuring the Time Threshold for an RNS Instance

Command	**threshold** *milliseconds*
Parameter Description	*milliseconds:* Indicates the time threshold for the test. The value ranges from 0 to 60,000, in the unit of milliseconds. The default value is 5,000.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo)
Usage Guide	Configure the threshold based on the following formula to ensure correct test calculation. (**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *milliseconds*)

Configuring the Time Threshold for an RNS Instance

Command	**timeout** *millisecond*
Parameter Description	*millisecond*: Indicates the test timeout. The value ranges from 10 to 604,800,000. The unit is ms. The default timeout varies according to the test type.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo)
Usage Guide	Configure the timeout based on the following formula to ensure correct test calculation. (**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *milliseconds*)

Configures the TOS Field in the IPv4 Header of Test Packets

Command	**tos** *number*
Parameter Description	*number*: Sets the TOS field in the IPv4 header of test packets. The value ranges from 0 to 255. The default value is 0.
Command	IP RNS DNS configuration mode (config-ip-rns-dns)

Mode	IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo)
Usage Guide	TOS is a 8-bit field in the IPv4 packet header. By setting the TOS, you can control the priority of the test packet. For different TOS fields, the processing priorities are different on the intermediate routers.

Configuration Example

Scenario **Figure 2- 5**	
Configuration Steps	Configure RNS instance 1 and related parameters on Switch A.
Switch A	A# configure terminal A(config)# ip rns 1 A(config-ip-rns)# dns www.fs.com.cn name-server 10.2.2.2 A(config-ip-rns-dns)#exit A(config)ip rns schedule 1 start-time now life forever
Verification	Run the **show ip rns configuration** command to display the instance configurations.
Switch A	A#show ip rns configuration 1 Entry number: 1 Tag: Type of operation to perform: dns Operation timeout (milliseconds): 5000 Operation frequency (milliseconds): 60000 Threshold (milliseconds): 5000 Recurring (Starting Everyday): FALSE Life (seconds): forever Next Scheduled Start Time:Start Time already passed Target host name: www.fs.com.cn Name Server: 10.2.2.2

Common Errors

- The DNS IP address is incorrect.

2.4.4 Configuring the Track Support for the RNS

Configuration Effect

- Configure the track function to track the test result of an RNS instance.

- Configure the track function to track the link status of an interface.
- Configure the track function to track the status of a track list.
- Configure the track function to track the status of an RNS list.

Notes

- To configure the track function to track the test result of an RNS instance, you need to configure the related RNS instance.
- To configure the track function to track the link status of an interface, you need to configure the related interface.
- To configure the track function to track the status of a track list, you need to configure the members for the related track list.
- To configure the track function to track the status of an RNS list, you need to configure the members for the related RNS list.

Configuration Steps

Configuring a Track Object

- Perform this operation if it is required to create a track object.
- The following four methods are available to create a track object:
  - Create a track object for tracking the test result of an RNS instance: Perform this configuration on every switching device unless otherwise required.
  - Create a track object for tracking the link status of an interface: Perform this configuration on every switching device unless otherwise required.
  - Create a track object for tracking the status of a track list: Perform this configuration on every switching device unless otherwise required.
  - Create a track object for tracking the status of an RNS list: Perform this configuration on every switching device unless otherwise required.

Configuring the Notification Delay of a Track Object

- Perform this configuration if it is required to delay notification of the status change of a track object.
- Delay for notifying the status change of a track object includes the delay for notifying the status change of a track object from UP to DOWN and the delay for notifying the status change of a track object from DOWN to UP. You can configure either delay or both of delays.
- Perform this configuration on every switching device unless otherwise required.

Configuring a Track Member

- Perform this configuration if it is required to configure a track object for tracking the status of a track list.
- When configuring a track member, you can set the status of a member meeting conditions to UP or DOWN.
- Perform this configuration on every switching device unless otherwise required.

Verification

Observe the status of a track object when the status of the track object (such as test results of an RNS instance, link status of an interface, or status of a track list) changes.

- After the preset delay, run the **show track** command to check whether the current track status changes.

Related Commands

Configuring a Track Object for Tracking the Link Status of An Interface

Command	**track** *object-number* **interface** *interface-type interface-number* **line-protocol**
Parameter Description	*object-number*: Indicates the number of a track object. The value ranges from 1 to 700. *Interface-type interface-number*: Indicates the interface type and interface number.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure a track object for tracking the link status of an interface. When the link status of the interface is UP, the status of the corresponding track object is UP.

Configuring a Track Object for Tracking the Test Result of an RNS Test

Command	**track** *object-number* **rns** *entry-number*
Parameter Description	*object-number*: Indicates the number of a track object. The value ranges from 1 to 700. *entry-number*: Indicates the number of an RNS instance. The value ranges from 1 to 500.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure a track object for tracking the result of an RNS test. If the test succeeded, the track object is in Up state.

Configuring a Track Object for Tracking the Status of a Track List

Command	**track** *object-number* **listboolean** { **and** | **or** }
Parameter Description	*object-number*: Indicates the number of a track object. The value ranges from 1 to 700.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure a track object for tracking the status of a track list. The result can be the AND or OR operation result of all member status.

Configuring a Track Member

Command	**object** *object-number*[**not**]
Parameter Description	*object-number*: Indicates the number of a track object. The value ranges from 1 to 700.
Command Mode	Track configuration mode
Usage Guide	Run this command to configure a member for a track list. The number of track list members that can be configured is restricted only by the capacity of track objects.

Configuring the Notification Delay of a Track Object

Command	**delay** { **up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds* }
Parameter Description	**up** *seconds*: Specifies the delay for notifying the status change of a track object from DOWN to UP. The value ranges from 0 to 180. The unit is second. The default value is 0. **down** *seconds*: Specifies the delay for notifying the status change of a track object from UP to DOWN. The value ranges from 0 to 180. The unit is second. The default value is 0.

Command Mode	Track configuration mode
Usage Guide	When the status of a track object frequently changes, the status of the client that use this track object will frequently change as well. Using this command can delay notification of the status change of a track object. For example, if the status of a track object changes from UP to DOWN, and **delay down 10** is configured, the DOWN status of the track object is notified 10s later. If the status of the track objects changes to UP again within this period of time, no notification is sent. For the client that uses this track object, the status of the track object is always UP.

Displaying the Track Object Statistics

Command	**show track** [*object-number*]
Parameter Description	*object-number*: Indicates the number of a track object. The value ranges from 1 to 700. The default is all track objects.
Command Mode	Privileged EXEC mode
Usage Guide	Run this command to display statistics of track objects.

Configuration Example

Configuring Track Object3 for Tracking the Link Status of the Interface FastEthernet 1/0

Configuration Steps	● Configure a track object for tracking the link status of an interface. ● Configure the delay for notifying the status change from UP to DOWN.
	FS# configure terminal FS(config)# track 3 interface FastEthernet 1/0 line-protocol FS(config-track)# delay down 10 FS(config-track)# exit
Verification	Change the link status of the interface FastEthernet 1/0 to DOWN. ● Immediately check the status of the track object, and verify that the status is still UP. ● Check the status of the track object 10s later, and verify that the status changes to DOWN.
	FS# show track 3 Track 3 Interface FastEthernet 1/0 The state is Up, delayed Down (5 secs remaining) 1 change, current state last: 300 secs Delay up 0 secs, down 10 secs

Configuring Track Object 3 (When the status of track object 1 is UP, and the status of track object 2 is DOWN, the status of track object 3 is UP.)

Configuration Steps	● Configuring track object 1 and track object 2. ● Configure track object 3, and its members include track object 1 and track object 2.

	FS # config FS(config)#track 1 interface gigabitEthernet 0/0 line-protocol FS(config-track)#delay up 20 down 40 FS(config-track)#exit FS(config)# FS(config)#track 2 interface gigabitEthernet 0/1 line-protocol FS(config-track)#delay down 30 FS(config-track)#exit FS(config)# track 3 list Boolean and FS(config-track)#object 1 FS(config-track)#object 2 not FS(config-track)# exit
Verification	When the status of track objects 1 and 2 change, check the status of track object 3. ● When the status of track object 1 changes from DOWN to UP, and the status of track object 2 remains DOWN, verify that the status of track object 3 changes from DOWN to UP. ● When the status of track object 1 remains UP, and the status of track object 2 changes from DOWN to UP, verify that the status of track object 3 changes from UP to DOWN.
	FS# show track 3 Track 3 List boolean and Object 1 Object 2 not The state is Down 1 change,current state last:10 secs Delay up 0 secs,down 0 secs

Configuring Track Object 5 for Tracking the Test Result of RNS Instance 7

Configuration Steps	● Configure an RNS test. ● Configure a track object to track the result of the RNS test. ● Configure the delay for notifying the test result change from successful to unsuccessful, and the delay for notifying the test result change from unsuccessful to successful.
	FS# configure terminal FS (config)#ip rns 7 FS (config-ip-rns)#icmp-echo 2.2.2.2

	FS (config-ip-rns-icmp-echo)#exit FS (config)#ip rns schedule 7 start-time now life forever FS(config)# track 5 rns 7 FS (config-track)# delay up 20 down 30 FS (config-track)# exit
Verification	Let the test result of RNS instance 7 change from successful to unsuccessful. ● When the test result changes to unsuccessful, immediately check the status of track object 7, and verify that the status is still UP. ● Check the status of the track object 30s later, and verify that the status changes to DOWN.
	FS# show track 5 Track 5 Reliable Network Service 7 The state is Down 2 change, current state last: 10 secs Delay up 20 secs, down 30 secs

Configuring Track Object 5 for Tracking the Test Results of an RNS List (consisting of RNS Instances 1, 2–5, and 8)

Configuration Steps	● Configure and start an RNS test (see "RNS Configuration"). ● Configure a track object for tracking the test result of an RNS list. ● Configure the delay for notifying the test result change from UP to DOWN, and the delay for notifying the test result change from DOWN to UP.
	FS(config)# track 5 rns-list 1,2-5,8 and FS (config-track)# delay up 20 down 30 FS (config-track)# exit
Verification	Let the test result of one of the RNS instances 1, 2-5, and 8 changes from successful to unsuccessful. ● When the test result changes to unsuccessful, immediately check the status of track object 7, and verify that the status is still UP. ● Check the status of the track object 30s later, and verify that the status changes to DOWN.
	FS# show track 5 Track 5 rns-list 1,2-5,8 and The state is Down 2 change, current state last: 10 secs Delay up 20 secs, down 30 secs

Common Errors

- The track object for tracking an RNS test is configured, but the RNS test is not configured.
- The track object for tracking the link status of an interface is configured, but the corresponding interface is not configured.
- The track object for tracking the status of a track list, but no member of the RNS list is configured.
- The track object configured for tracking an RNS list, but the RNS test is not configured.

2.5 Monitoring

Displaying

Description	Command
Displays configurations of one or more RNS instances.	**show ip rns configuration** [*operation-number*]
Displays detailed statistics of one or more RNS instances.	**show ip rns collection-statistics** [*operation-number*]
Displays the current RNS status.	**show ip rns operational-state** [*operation-number*]
Displays the proactive threshold monitoring information of one or more RNS instances.	**show ip rns reaction-configuration** [*operation-number*]
Displays information about the test triggered by one or more RNS instances.	**show ip rns reaction-trigger** [*operation-number*]
Displays the brief statistics of one or more RNS instances.	**show ip rns statistics** [*operation-number*]
Displays the brief statistics of one or more track objects.	**show track** [*object-number*]
Displays the brief statistics of a track client.	**show track client**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the track module.	**debug track** { **all** | **proc-event** | **rdnd-event** | **client** }
Debugs the RNS module.	**debug rns** { **all** | **interface** | **lib** | **rdnd-event** | **restart** | **rns_id** [**0, 500**] }

Chapter 10 Routing Configuration

1. Configuring PBR
2. Configuring ROUTE-DB
3. Configuring RIP
4. Configuring RIPNG
5. Configuring OSPFv2
6. Configuring OSPFv3
7. Managing Routes

1 Configuring PBR

1.1 Overview

Policy-based routing (PBR) is implemented by applying a route map including policies to interfaces and devices.

Similar to static routing, PBR is also manually configured and cannot automatically update with network changes. In addition, PBR is effective only for packets sent from local interfaces and devices. As compared with static and dynamic routing, PBR is more flexible. Static and dynamic routing can forward packets only based on destination addresses. PBR can forward packets based on source and destination addresses, packet length and input interface.

1.2 Applications

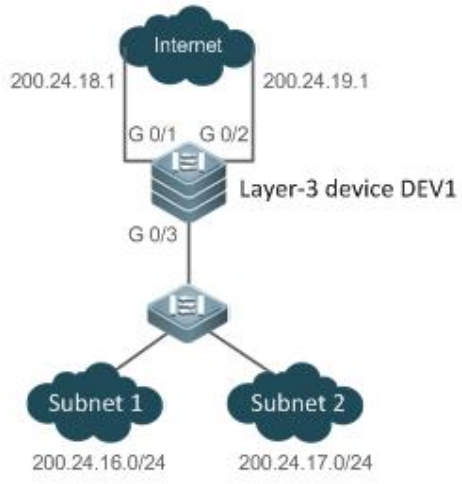
Application	Description
Selecting an ISP by Using PBR	Specify preferential output interfaces for packets from different subnets.
Implementing Traffic Classification by Using PBR	Specify QoS values for packets from different subnets.

1.2.1 Selecting an ISP by Using PBR

An existing user network often uses resources of multiple internet server providers (ISPs). PBR needs to be used since different bandwidths may be requested from different ISPs or the network resources for key users need to be protected. By controlling forwarding of certain data packets, you can make full use ISP resources as well as meet the requirements of flexible and diversified applications.

Scenario

Figure 1- 1



A LAN has two output interfaces for connecting the Internet. PBR is configured on the layer-3 device DEV1 to enable the two output interfaces to implement load sharing and mutual backup.

The specific requirements are as follows:

- Data streams from subnet 1 are sent from GE 0/1.

- Data streams from subnet 2 are sent from GE 0/2.
- If the GE 0/1 link is disconnected, the data streams on GE 0/1 are switched to GE 0/2. Vice versa.

Deployment

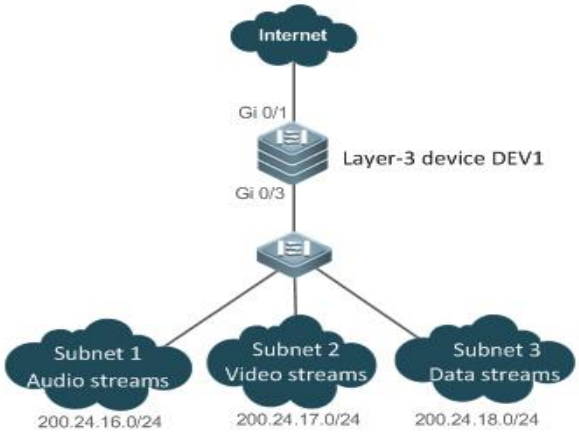
- Configure two different ACLs on the layer-3 device DEV1:
- ACL1: source addresses belong to subnet 1.
- ACL2: source addresses belong to subnet 2.
- Configure two policies in the route map on the layer-3 device DEV1:
- Policy 1: sets the next hops for packets matching ACL1 to GE0/1 and GE0/2 (Based on the configuration sequence, GE0/1 takes effect first and GE0/2 works in the backup mode).
- Policy 2: sets the next hops for packets matching ACL2 to GE0/2 and GE0/1 (Based on the configuration sequence, GE0/2 takes effect first and GE0/1 works in the backup mode).
- Configure PBR on GE0/3 (by using a route map). Then, packets received on this interface are forwarded based on the policies.

1.2.2 Implementing Traffic Classification by Using PBR

Scenario

Networks of medium- and small-sized enterprises have simple structures. Different branch nodes are interconnected to the central nodes through carrier dedicated lines or the Internet VPN mode. Enterprise networks often need to implement three-in-on integration (of audio, video and data) to maximize the utilization of existing IP networks and save costs. Since all traffic is output from a single output interface, it is necessary to adjust the QoS policies for the output interface, in order to provide preferential communication quality for bandwidth- and delay-sensitive applications.

Figure 1- 2



A LAN has an output interface for connecting the Internet. PBR is configured on the layer-3 device DEV1 to change the QoS values for packets from different networks.

The specific requirements are as follows:

- For data streams from subnet 1, representing audio streams, set the DSCP value to 56.
- For data streams from subnet 2, representing video streams, set the DSCP value to 40.
- For data streams from subnet 3, representing data streams, set the DSCP value to 24.

Deployment

- Configure three different ACLs on the layer-3 device DEV1:

  ACL1: source addresses belong to subnet 1.

  ACL2: source addresses belong to subnet 2.

  ACL3: source addresses belong to subnet 3.

- Configure three policies in the route map on the layer-3 device DEV1:

  Policy 1: sets the DSCP value for packets matching ACL1 to 56.

  Policy 2: sets the DSCP value for packets matching ACL2 to 40.

  Policy 3: sets the DSCP value for packets matching ACL3 to 24.

- Configure PBR on GE0/3 (by using a route map). Then, the DSCP values for packets received on this interface are changed based on the policies.

1.3 Features

Feature	Description
Configuring a Policy	Before configuring PBR, configure policies in a route map.
Configuring PBR	Apply a route map including policies to interfaces and devices to implement PBR.

1.3.1 Configuring a Policy

A policy is a "match …, set…" statement, which indicates that "if certain conditions are matched, perform certain processing actions".

For detailed introduction to the policies, see the section "Route Map".

Executing Policies

In the global configuration mode, you can run the **route-map** *route-map-name* [**permit** | **deny**] [*sequence-number*] command to create a policy in a route map.

A route map may contain multiple policies. Each policy has a corresponding sequence number. A smaller sequence number means a higher priority. Policies are executed based on their sequence numbers. Once the matching condition of a policy is met, the processing action for this policy needs to be executed and the route map exits. If no matching condition of any policy is met, no processing action will be performed.

Policies have two working modes:

- permit: When the matching condition of a policy is met, perform the processing action for this policy and exit the route map.
- deny: When the matching condition of a policy is met, do not perform the processing action for this policy and exit the route map.

Matching conditions of policies

The matching conditions of a policy may contain 0, 1 or more matching rules.

- If 0 matching rule is contained, no packet will be matched.
- If one or more match rules are contained, all match rules must be matched at the same time to meet the matching conditions of the policy.

In the route map mode, run the **match** command to configure match rules. One **match** command is mapped to one match rule.

PBR supports the following **match** commands:

	Command	Description
IPv4 PBR	**match length**	The IPv4 packet length is used as the matching condition. Only one **match length** command can be configured in a policy.
	match ip address	The source IPv4 address (and the destination IPv4 address) is used as the matching condition. Multiple **match ip address** commands can be configured in a policy.

IPv4 PBR defines the source IP address (and destination IP address) ranges of packets by using the IP standard or extended ACLs.

When PBR uses an ACL that is unavailable, the route sub-map will not be matched and the next route sub-map will be matched instead. If no route sub-map is matched, a common route will be selected for forwarding. If only ACLs are configured but no ACE is configured, the PBR forwarding behavior is the same as that in a scenario where an ACL is unavailable.

Processing action for a policy

The processing action of a policy may contain 0, 1 or more set rules.

- If 0 set rule is contained, no processing action will be performed and the route map will directly exit.
- If one or more set rules are contained, all processing actions will be performed and the route map will exit.

If set rules have different priorities, the set rule with the highest priority will take effect.

In the route map mode, run the **set** command to configure set rules. One **set** command is mapped to one set rule.

PBR supports the following **set** commands:

	Command	Description
IPv4 PBR	**set ip tos**	Modifies the **tos** field of an IPv4 packet. This command cannot work with the **set ip dscp** command.
	set ip precedence	Modifies the **precedence** field of an IPv4 packet. This command cannot work with the **set ip dscp** command.
	set ip dscp	Modifies the **dscp** field of an IPv4 packet. This command cannot work with the **set ip tos** and **set ip precedence** commands.

The priority sequence is as follows: **set ip next-hop** > **set interface** > common route > **set ip default next-hop** > **set default interface** > default route. The preceding **set** commands can be configured at the same time but only the command with the highest priority takes effect.

1.3.2 Configuring PBR

PBR

Apply a route map including policies to interfaces or devices to implement PBR.

- Apply a route map to an interface so that packets received by the interface are routed based on the policy.
- The PBR is often used to control user packets received by a device. This command is effective only for forwarded packets, but not for locally initiated packets.
- Apply a route map to a device so that packets locally initiated are routed based on the policy.
- The PBR is often used to control protocol packets exchanged between devices (such as ping packets sent locally). This command is effective only for locally initiated packets, but not for forwarded packets.

By default, PBR is not unavailable on a device and packets are forwarded based on a routing table.

Redundant backup or load balancing

You can set multiple next hops in a policy. Either redundant backup or load balancing can be implemented among multiple next hops. Redundant backup is implemented by default.

Redundant backup or load balancing is only effective for next hops configured in the **set ip next-hop**, **set ip next-hop recursive** and **set ip default next-hop** commands, and only effective among multiple next hops in the same set rule.

- Redundant backup
- Based on the configuration sequence, the first accessible next hop takes effect. When the currently effective next hop (R1) is faulty, the traffic automatically switches to the next accessible next hop (R2). When R1 becomes accessible again, the traffic automatically switches back to R1.
- A newly added next hop is arranged at the last of the sequence. Assume that the original sequence of multiple next hops is R1 > R2 > R3. After R1 is deleted and added again, the sequence changes to R2 > R3 > R1.
- If no next hop is accessible, packets will be discarded.
- Load balancing
- When multiple accessible next hops take effect at the same time, the Weighted Cost Multiple Path (WCMP) and Equal Cost Multiple Path (ECMP) are supported. After an accessible next hop loses effect, traffic will be balanced among the other accessible next hops.

Correlation with Track

Correlation between PBR and Track is effective only for next hops configured by the **set ip next-hop** command.

The **set ip next-hop** command carries the **verify-availability** and **track** *track-obj-number* parameters, which can establish correlation between PBR and a Track session and monitor the accessibility of next hops.

Correlation between PBR and Track helps enhance the PBR's perception about network environment changes. When Track detects that the current next hop is not accessible, the Track will immediately notify the PBR to switch the traffic to another accessible next hop (to implement redundant backup) or all the other accessible next hops (to implement load balancing).

Only IPv4 PBR supports correlation with Track.

For the configuration and related commands for correlation between PBR and Track, see the "RNS" section.

1.4 Configuration

Configuration	Description and Command
Configuring Basic Functions of PBR	(Mandatory) It is used to apply PBR to forward packets.

Configuration	Description and Command	
	ip policy route-map	Applies PBR for IPv4 packets received by an interface.
	ip local policy route-map	Applies PBR for IPv4 packets locally initiated.
Setting Redundant Backup or Load Balancing	(Optional) It is used to set whether PBR implements redundant backup or load balancing among multiple next hops.	
	ip policy { **redundance** | **load-balance** }	Sets whether IPv4 PBR implements redundant backup or load balancing among multiple next hops. The default setting is redundant backup.

1.4.1 Configuring Basic Functions of PBR

Configuration Effect

Perform personalized routing management for user data streams by preparing flexible policies.

Perform personalized management for protocol interaction and network topologies by preparing flexible policies.

Notes

- A route map must be used when PBR is configured; therefore, you must configure a route map on a device.
- If an ACL is used when the route map is configured, you must configure the ACL on the device.

Configuration Steps

Applying PBR for IPv4 packets received by an interface

- To perform personalized routing management for IPv4 user data streams passing a device, you should perform this configuration.
- Perform this configuration on the input interface for user data streams.
- Run the **ip policy route-map** command to apply a route map to an interface. Then, PBR is executed for IPv4 packets received on this interface.

Command	**ip policy route-map** *route-map-name*
Parameter Description	*route-map-name*: Indicates the name of a route map.
Defaults	By default, PBR is unavailable on a device and packets are forwarded based on a routing table.
Command Mode	Interface configuration mode
Usage Guide	Only one **ip policy route-map** command can be configured for an interface. If multiple **ip policy route-map** commands are configured for an interface, only the last configuration takes effect. If the route map used in PBR is unavailable, the PBR does not take effect.

Applying PBR for IPv4 packets locally initiated

- To perform personalized management for IPv4 protocol interaction and IPv4 network topologies, you should perform this configuration.

- Run the **ip local policy route-map** command to apply a route map to a device. Then, PBR is executed for IPv4 packets locally initiated.

Command	**ip local policy route-map** *route-map-name*
Parameter Description	*route-map-name*: Indicates the name of a route map.
Defaults	By default, PBR is unavailable on a device and packets are forwarded based on a routing table.
Command Mode	Global configuration mode
Usage Guide	Only one **ip local policy route-map** command can be configured for a device. If the route map used in PBR is unavailable, the PBR does not take effect.

Verification

- Check the configurations of PBR.
- Check the configurations of the route map used by PBR.
- If an ACL is used when the route map is configured, you should check the configurations of the ACL.

Checking the configurations of IPv4 PBR

Command	**show ip policy** [*route-map-name*]
Parameter Description	*route-map-name*: Indicates the name of a route map.
Command Mode	Privilege, global and interface configuration modes
Usage Guide	Check the interfaces configured with IPv4 PBR according to the output information and the name of the used route map. FS# show ip policy Banlance mode: redundance Interface Route map local RM_for_PBR_1 GigabitEthernet 0/1 RM_for_PBR_2 **Local** indicates applying policy-based routing for IPv4 packets locally initiated.

Checking the configurations of a route map

Command	**show route-map** [*route-map-name*]
Parameter Description	*route-map-name*: Indicates the name of a route map.
Command Mode	Privilege, global and interface configuration modes
Usage Guide	Multiple route maps may be available on a device. Focus on the route map used in PBR and check its policy settings. FS# show route-map route-map RM_FOR_PBR, permit, sequence 10 Match clauses: ip address acl1

	Set clauses: ip next-hop 200.24.18.1 route-map RM_FOR_PBR, permit, sequence 20 Match clauses: ip address acl2 Set clauses: ip next-hop 200.24.19.1

Checking the configurations of an ACL

Command	**show access-lists** [*acl-id* | *acl-name*]
Parameter Description	*acl-id*: Indicates the ACL ID. *acl-name*: Indicates the ACL name.
Command Mode	Privilege, global and interface configuration modes
Usage Guide	Multiple ACLs may be available on a device. Focus on the ACL used by a route map and check its configurations. FS# show access-lists 1 ip access-list standard 1 10 permit 200.24.16.0 0.0.0.255 ip access-list standard 2 10 permit 200.24.17.0 0.0.0.255

Checking the routing information of IPv4 PBR

Command	**show ip pbr route** [**interface** *if-name* | **local**]
Parameter Description	*if-name*: Indicates an interface name. **local**: Indicates local.
Command Mode	Privilege, global and interface configuration modes
Usage Guide	Specify a local interface or device and check the routing information of IPv4 PBR. FS# show ip pbr route PBR IPv4 Route Summay : 1 Interface : GigabitEthernet 0/1 Sequence : 10 Min Length : None Max Length : None VRF ID : 0 Route Flags : Route Type : PBR

```
  Direct            : Permit
  Priority          : High
  Tos_Dscp          : None
  Precedence        : None
Tos_Dscp            : 0
Precedence          : 0
Mode                : redundance
Nexthop Count       : 1
  Nexthop[0]        : 192.168.8.100
  Weight[0]         : 1
  Ifindex[0]        : 2
```

Checking a route map used by IPv4 PBR

Command	**show ip pbr route-map** *rmap-name*
Parameter Description	*rmap-name*: Indicates the route map name.
Command Mode	Privilege, global and interface configuration modes
Usage Guide	Specify a route map and check the route map used by IPv4 PBR.

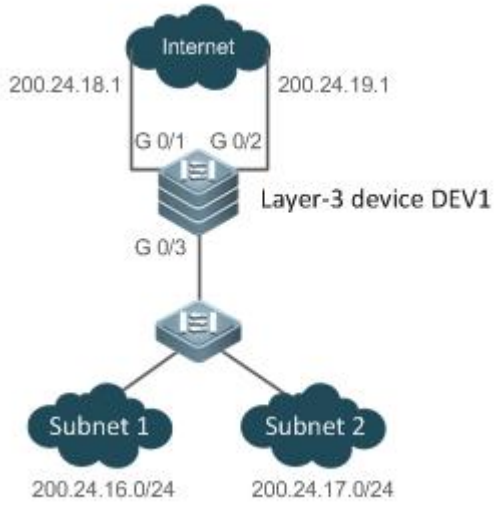
```
FS# show ip pbr route-map rm
PBR VRF: GLOBAL, ID: 0
  Forward Mode: redundance
  Forwarding: On

Route-map rm
  Route-map index: Sequence 10, permit
    Match rule:
      ACL ID :     2900, CLS: 1, Name: acl1
    Set rule:
      IPv4 nexthop: 192.168.8.100, (VRF name: , ID: 0), Weight: 0
        PBR state info ifx: 2, Connected: True, Track state: Up
```

Checking the statistics about packets forwarded by IPv4 PBR

Command	**show ip pbr statistics** [**interface** *if-name* | **local**]
Parameter Description	*if-name*: Indicates an interface name. **local**: Indicates local.
Command	Privilege, global and interface configuration modes

Mode	
Usage Guide	FS# show ip pbr statistics IPv4 Policy-based route statistic gigabitEthernet 0/1 statistics : 10

Configuring correlation between IPv4 PBR and Track

Scenario Figure 1- 3	
	The layer-3 device DEV 1 is connected to subnet 1 and subnet 2 through GE0/3. The network segment where subnet 1 resides is 200.24.16.0/24 whereas the network segment where subnet 2 resides is 200.24.17.0/24. DEV 1 is connected to the Internet through GE0/1 and GE0/2 and their next hops are 200.24.18.1 and 200.24.19.1.
	● DEV1 can fast detect a faulty output link and switch to a backup link.
Configuration Steps	When configuring IPv4 PBR and selecting an output link based on source addresses of the packets, add or modify the following configurations (red fields): ● Set two Track objects and track the accessibility of the next hops of the two output interfaces. ● When configuring a policy, set the correlation between the next hops and the Track objects.
DEV1	DEV1(config)# ip access-list extended 101 DEV1(config-ip-acl)# permit ip 200.24.16.0 0.0.0.255 any DEV1(config-ip-acl)# exit DEV1(config)# ip access-list extended 102 DEV1(config-ip-acl)# permit ip 200.24.17.0 0.0.0.255 any DEV1(config-ip-acl)# exit DEV1(config)#ip rns 1 DEV1(config-ip-rns)#icmp-echo 200.24.18.1 DEV1(config)#ip rns schedule 1 start-time now life forever

	DEV1(config)#track 1 rns 1 DEV1(config)#ip rns 2 DEV1(config-ip-rns)#icmp-echo 200.24.19.1 DEV1(config)#ip rns schedule 2 start-time now life forever DEV1(config)#track 2 rns 2 DEV1(config)# route-map RM_FOR_PBR 10 DEV1(config-route-map)# match ip address 101 DEV1(config-route-map)# set ip next-hop verify-availability 200.24.18.1 track 1 DEV1(config-route-map)# set ip next-hop verify-availability 200.24.19.1 track 2 DEV1(config-route-map)# exit DEV1(config)# route-map RM_FOR_PBR 20 DEV1(config-route-map)# match ip address 102 DEV1(config-route-map)# set ip next-hop verify-availability 200.24.19.1 track 2 DEV1(config-route-map)# set ip next-hop verify-availability 200.24.18.1 track 1 DEV1(config-route-map)# exit DEV1(config)# interface GigabitEthernet 0/3 DEV1(config-if-GigabitEthernet 0/3)# ip policy route-map RM_FOR_PBR DEV1(config-if-GigabitEthernet 0/3)# exit DEV1(config)# ip policy redundance
Verification	● Check whether the Track objects are up.
DEV1	DEV1#show track Track 1 Reliable Network Service 1 The state is Up 1 change, current state last: 120 secs Delay up 30 secs, down 50 secs Track 2 Reliable Network Service 2 The state is Up 1 change, current state last: 130 secs Delay up 30 secs, down 50 secs

Common Errors

- A route map is used when PBR is configured but the route map does not exist.

- An ACL is used when a route map is configured but the ACL does not exist.

1.4.2 Setting Redundant Backup or Load Balancing

Configuration Effect

- Using multiple next hops in the mutual backup mode can enhance the network reliability.
- Implementing load balancing among multiple next hops can expand the network bandwidth.

Notes

- The basic functions of PBR must be configured.
- Redundant backup and load balancing are effective only for the next hops set by the following **set** commands.

Command	Description
set ip next-hop	Configures the next hop of IPv4 packets. This command carries the *weight* parameter, which is used to set the weight of the WCMP. The default value is 1.
set ip default next-hop	Configures the default next hop of IPv4 packets. This command carries the *weight* parameter, which is used to set the weight of the WCMP. The default value is 1.

Up to eight next hops can be set for WCMP whereas up to 32 next hops can be set for ECMP.

Configuration Steps

Setting whether IPv4 PBR implements redundant backup or load balancing among multiple next hops

- If load balancing needs to be implemented among multiple next hops, this configuration needs to be performed.
- If load balancing is configured at present, you also need to perform this configuration to reset redundant backup.
- This configuration is effective for all PBRs configured on a device.

Command	**ip policy** { **redundance** | **load-balance** }
Parameter Description	redundance: Indicates redundant backup. load-balance: Indicates load balancing.
Defaults	Redundant backup is configured by default.
Command Mode	Global configuration mode
Usage Guide	If redundant backup is selected, the first next hop takes effect based on the configuration sequence. If load balancing is selected, all next hops take effect at the same time and share traffic by weight.

Verification

- Check whether redundant backup or load balancing is implemented among multiple next hops.

Checking whether IPv4 PBR implements redundant backup or load balancing among multiple next hops

Command	**show ip policy** [*route-map-name*]
Parameter Description	***route-map-name*: Specifies a route map.**
Command Mode	Privilege, global and interface configuration modes

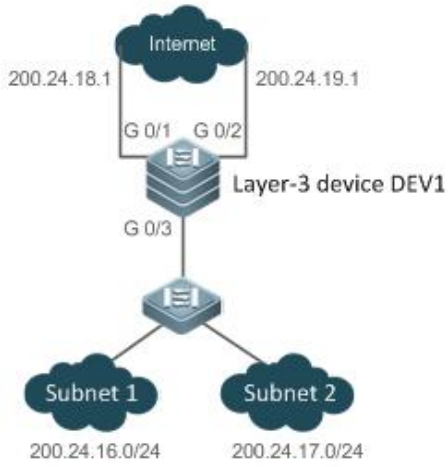
Usage Guide	See the following example and focus on the red field. FS# show ip policy Banlance mode: redundance Interface Route map local test GigabitEthernet 0/3 test

Configuration Example

Configuring IPv4 PBR to implement redundant backup among multiple next hops

See the preceding example: Configuring IPv4 PBR and selecting an output link based on source addresses of packets

Configuring IPv4 PBR to implement load balancing among multiple next hops

Scenario **Figure 1-4**	
	The layer-3 device DEV 1 is connected to subnet 1 and subnet 2 through GE0/3. The network segment where subnet 1 resides is 200.24.16.0/24 whereas the network segment where subnet 2 resides is 200.24.17.0/24. DEV 1 is connected to the Internet through GE0/1 and GE0/2 and their next hops are 200.24.18.1 and 200.24.19.1.
	This LAN has two output interfaces for connecting the Internet. The requirements are as follows: The traffic is equally shared by GE0/1 and GE0/2.
Configuration Steps	● Configure basic functions of PBR. Specify multiple next hops. ● Set the load balancing mode.
	DEV1(config)# route-map RM_LOAD_PBR 10 DEV1(config-route-map)# set ip next-hop 200.24.18.1 DEV1(config-route-map)# set ip next-hop 200.24.19.1 DEV1(config-route-map)# exit DEV1(config)# interface GigabitEthernet 0/3

	DEV1(config-if-GigabitEthernet 0/3)# ip policy route-map RM_LOAD_PBR DEV1(config-if-GigabitEthernet 0/3)# exit DEV1(config)# ip policy load-balance
Verification	● Check the configurations of IPv4 PBR. ● Check the configurations of the route map.
	DEV1# show ip policy Balance mode: load-balance Interface Route map GigabitEthernet 0/3 RM_LOAD_PBR
	DEV1# show route-map route-map PBR-VRF-Selection, permit, sequence 10 Match clauses: Set clauses: ip next-hop 200.24.18.1 8 ip next-hop 200.24.19.1 8

1.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears the statistics about packets forwarded by IPv4 PBR.	**clear ip pbr statistics** [**interface** *if-name* | **local**]

Displaying

Description	Command
Displays the configurations of IPv4 PBR.	**show ip policy**
Displays the configurations of a route map.	**show route-map** [*name*]
Displays the configurations of an ACL.	**show access-list**
Displays the routing information of IPv4 PBR.	**show ip pbr route** [**interface** *if-name* | **local**]
Displays a route map used by IPv4 PBR.	**show ip pbr route-map** *rmap-name*
Displays the statistics about IPv4 PBR.	**show ip pbr statistics** [**interface** *if-name* | **local**]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs PBR errors.	**debug pbr error**

Description	Command
Debugs PBR events.	**debug pbr events**
Debugs multiple service cards supported by PBR.	**debug pbr ms**
Debugs PBR message communication.	**debug pbr msg**
Debugs interaction between PBR and NSM.	**debug pbr nsm**
Debugs packet forwarding of PBR.	**debug pbr packet**
Debugs PBR GR.	**debug pbr restart**

2 Configuring ROUTE-DB

2.1 Overview

ROUTE-DB is a feature for matching a route database in an environment with routes of multiple operators according to an external IP address accessed by a client. This feature can find out the most appropriate route type for packet forwarding, which reduces the probability of access across networks of multiple operators, and increases the speed of network access.

2.2 Applications

Application	Description
Applying Scenario with Routes of Multiple Operators	The network egress gateway accesses networks of different operators via different routes.

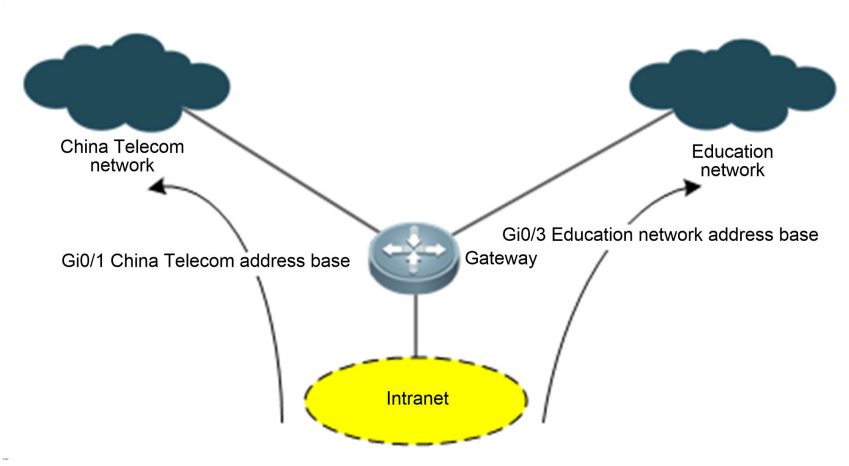
2.2.1 Applying Scenario with Routes of Multiple Operators

Scenario

The egress gateway connects to the China Telecom network and the education network via two different routes.

- The route dedicated for the China Telecom network is used to access data streams of China Telecom resources.
- The route dedicated for the education network is used to access data streams of education network resources.

Figure 2- 1



Deployment

- Configure different routes for different operators.

2.3 Features

Basic Concepts

↘ ISP

Internet Service Provider (ISP) refers to a telecom operator that provides Internet access services, information services, and value-added services for users.

When a user accesses a network resource across networks of different operators, the access speed is extremely slow and the user may even fail to access the resource.

Feature

Feature	Description
Route Database Routing	Matches a route database according to an external IP address accessed by the client to select the most appropriate route type for packet forwarding.
Route Database Update	Updates the route database.
User-defined Route Database	Users can add or delete a route database as needed.
Route Database Query	Queries the route database.

2.3.1 Route Database Routing

In a scenario with routes of multiple operators, the probability of access across networks of multiple operators is reduced, and the speed of network access is increased.

Working Principle

When a user accesses a network resource across networks of different operators, the access speed is extremely slow and the user may even fail to access the resource. Therefore, multiple routes are adopted for access in many places providing a network. This requires the egress gateway to automatically select a route type according to an external IP address accessed by the client, so as to forward packets. In such case, ROUTE-DB matches an external IP address, and based on different IP addresses, determines a route type for transmitting the data stream. In this way, ROUTE-DB ensures that no access across networks of different operators occurs, thereby improving user experience.

Each operator is assigned with a fixed network segment and information about the network segment division is recorded in the encrypted route database file. The egress gateway obtains this information and modifies the routing table, so as to control routing for data stream transmission.

Related Configuration

Configuring Route Database for Interface

No route database is configured for any interface by default.

Run the **route-auto-choose** command to configure a route database for an interface.

2.3.2 Route Database Update

A route database must be updated after information in the route database changes.

Working Principle

After address information of an operator network changes, the route database must be updated to generate a new route database file, which is sent to the gateway.

Related Configuration

Updating a Route Database

Run the **route-auto-choose update** command to update a route database.

2.3.3 User-defined Route Database

When routings in the system's route database cannot meet the user's needs, the user can configure a user-defined route database.

Working Principle

N/A

Related Operations

Configuring a User-defined Route Database

Run the **route-auto-choose user-defined** { **name** [*ip-address mask*] | **update** *file-path* } command to configure a user-defined route database. No database is configured by default.

2.3.4 Route Database Query

The administrator can query the route database to learn the number of operator types in the current route database file or determine whether an operator to which a certain IP address belongs.

Working Principle

Run a command to query operator types supported in the route database file. For a route database of an earlier version, information about China Mobile, China Telecom, China Unicom, and Education Network is returned by default. If the route database file contains level-2 operators, information about all operators is returned. Each IP address in the route database file corresponds to one operator, and can be obtained by querying the route database file.

Related Operations

Run the s**how route-db-info db-type** command to query operator types in the current route database file.

Run the **show route-db-info** *ip-address* command to query the operator to which an IP address belongs.

2.4 Configuration

Configuration	Description and Command	
Configure Route Database	Mandatory	
	route-auto-choose	Configure the route database type
Update Route Database	Optional	
	route-auto-choose update	Update a route database
Configure User-defined Route Database	Optional	
	route-auto-choose user-defined	Configure a user-defined route database

2.4.1 Configuring Route Database

Configuration Effect

- Configure a route database type so that traffic compliant with the route database is transmitted to the route corresponding to the route database.

Notes

- Generally, only one operator is configured for an outbound interface in a simple operator network. With more and more second-level operators, one second-level operator may belong to multiple first-level operators. As a result, load balancing cannot be performed based on the route database, affecting the load balancing effect on multiple outbound interfaces. Therefore, multiple operators can be configured for one interface, that is, one interface can be configured in multiple route types. For example, gigabitEthernet 0/1 can be configured for both the China Telecom and China Unicom route types.
- Different interfaces can be configured for a same route type. For example, gigabitEthernet 0/1 and gigabitEthernet 0/2 can both belong to the China Telecom route.

Configuration Steps

Configuring Route Database Type

- Mandatory.

Verification

Configure a certain interface for the China Telecom route.

- Access corresponding China Telecom resources to check whether the route is correctly selected.
- Run traceroute to check whether the route is correctly selected.

Related Commands

Configuring Route Database Type

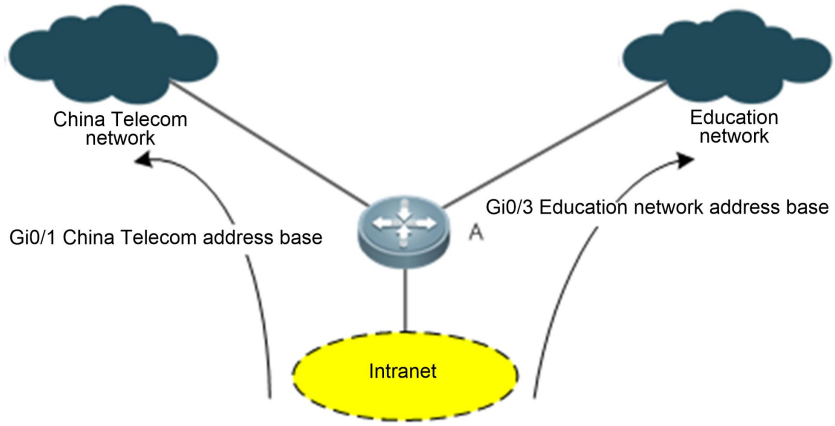
Command	[**no**] **route-auto-choose** {**cnc** | **cnii** | **cernet** | **cmcc** | *word*} *interface next-hop* [**tag** *num*] [*distance*]

Parameter Description	**cnc:** Indicates the China Unicom route database. **cnii:** Indicates the China Telecom route database. **cernet:** Indicates the route database of the education network. **cmcc:** Indicates the China Mobile route database. *word*: Configures other operator types except that of the preceding four operators. *interface*: Indicates the outbound interface corresponding to the route database. *next-hop*: Indicates the next-hop IP address of the router corresponding to the route database. **tag** *num*: Indicates the tag of the router corresponding to the route database. *distance*: Indicates the metric value for route database routing.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

The following example describes only configuration related to route databases.

Applying China Telecom Route Database on gigabitEthernet 0/1 and Education Network Route Database on gigabitEthernet 0/3

Scenario Figure 2-2	
Configuration Steps	● Apply the China Telecom route database on gigabitEthernet 0/1 and the China Network route database on gigabitEthernet 0/3.
A	A# configure terminal A(config)# route-auto-choose cnii gigabitEthernet 0/1 202.100.12.5 A(config)# route-auto-choose cernet gigabitEthernet 0/3 201.1.1.1
Verification	Access China Telecom resources from the intranet to check whether data stream is transmitted on a correct route. ● Run the **show** command to check whether the configuration is successful.
A	A# show run | i route-auto-choose route-auto-choose cnii gigabitEthernet 0/1 202.100.12.5 route-auto-choose cernet gigabitEthernet 0/3 201.1.1.1

Common Errors

- No corresponding outbound interface is configured.

- The interface is down after the route database is configured on it, and traffic destined for the route corresponding to the route database is directly discarded, instead of being transmitted on the default route.

2.4.2 Updating Route Database

Configuration Effect

- Update the latest route database version to the currently running system.

Configuration Steps

- Upload the latest route database version to the gateway.
- Run the route-auto-choose update command to update the route database on the gateway.

Verification

Check the route database version.

Related Commands

Updating Route Database

Command	**route-auto-choose update**
Parameter Description	**update:** Update the route database.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Updating Route Database

Configuration Steps	● Update the route database.
	FS# configure terminal FS(config)# route-auto-choose update FS(config)# end
Verification	Run the show route-db-info date command to check the version of route database.

Common Errors

- N/A

2.4.3 Configuring User-defined Route Database

Configuration Effect

- The user configures the name and other information of the route database as needed.

Configuration Steps

- Run the **route-auto-choose user-defined name** command to configure the route database as needed.

Verification

Run the **show route-db-info user-defined** command to check the information about the user-defined route database.

Related Commands

Configuring User-defined Route Database

Command	**route-auto-choose user-defined name** [*ip-address mask*]
Parameter Description	**Name**: name of the user-defined route database *ip-address*: IP addresses in the user-defined route database *mask*: masks in the user-defined route database
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Updating Route Database

Configuration Steps

- Update the route database

```
FS# configure terminal
FS(config)# route-auto-choose user-defined name test1 1.2.3.0 255.255.255.0
FS(config)# end
```

Verification

Run the **show route-db-info user-defined** command to check the information of the user-defined route database

```
FS#show route-db-info user-defined
test1:
  1.2.3.0 255.255.255.0
```

Common Errors

- N/A

2.5 Monitoring and Maintenance

N/A

3 Configuring RIP

3.1 Overview

Routing Information Protocol (RIP) is a unicast routing protocol applied on IPv4 networks. RIP-enabled routers exchange routing information to obtain routes to remote networks.

As an Interior Gateway Protocol (IGP), RIP can run only within the autonomous system (AS) and is applicable to small-sized networks whose longest path involves less than 16 hops.

Protocols and Standards

- RFC1058: Defines RIPv1.
- RFC2453: Defines RIPv2.

3.2 Applications

Application	Description
Basic RIP Application	The routing information is automatically maintained through RIP on a small-sized network.

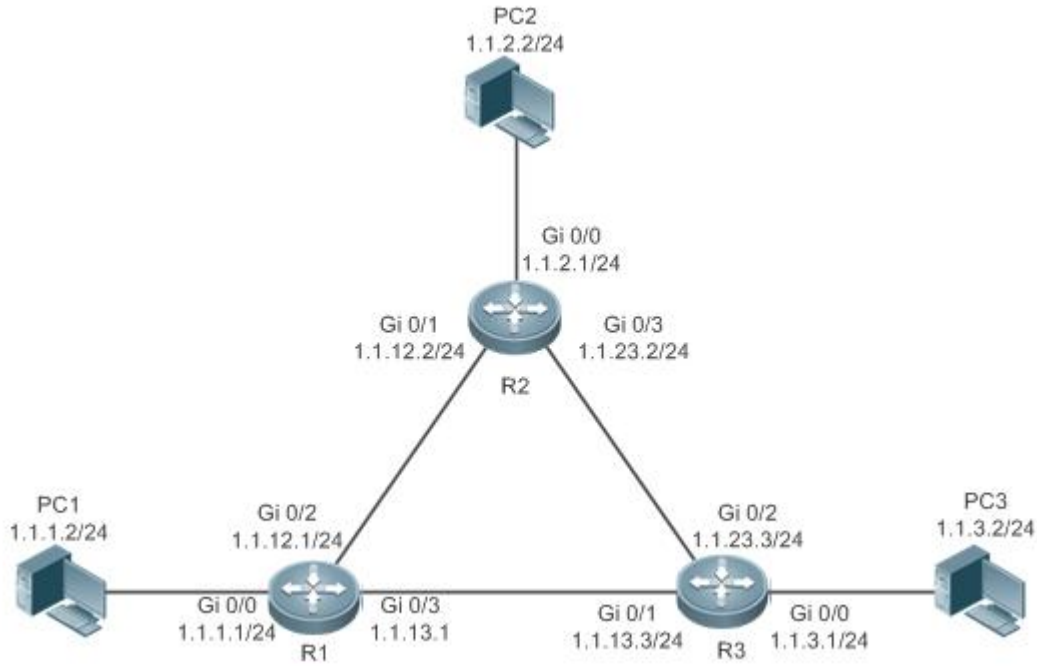
3.2.1 Basic RIP Application

Scenario

On a network with a simple structure, you can configure RIP to implement network interworking. Configuring RIP is simpler than configuring other IGP protocols like Open Shortest Path First (OSPF). Compared with static routes, RIP can dynamically adapt to the network structure changes and is easier to maintain.

As shown in Figure 2- 3- 1, to implement interworking between PC1, PC2, and PC3, you can configure RIP routes on R1, R2, and R3.

Figure 2- 3- 1



Deployment

- Configure IP addresses and gateways on three PCs.
- Configure IP addresses and subnet masks on three routers.
- Configure RIP on three routers.

3.3 Features

Basic Concepts

IGP and EGP

IGP runs within an AS. For example, RIP is a type of IGP.
Exterior Gateway Protocol (EGP) runs between ASs. For example, BGP is a type of EGP.

Classful Routing Protocol and Classless Routing Protocol

Protocols can be classified based on the type of routes supported:

- Classful routing protocol: It supports classful routes. For example, RIPv1 is a classful routing protocol.
- Classless routing protocol: It supports classless routes. For example, RIPv2 is a classless routing protocol.

Overview

Feature	Description
RIPv1 and RIPv2	RIP is available in two versions: RIPv1 and RIPv2.
Exchanging Routing Information	By exchanging routing information, RIP-enabled devices can automatically obtain routes to a remote network and update the routes in real time.
Routing Algorithm	RIP is a protocol based on the distance-vector algorithm. It uses the vector addition method to compute the routing information.
Avoiding Route Loops	RIP uses functions, such as split horizon and poison reverse, to avoid route loops.
Security Measures	RIP uses functions, such as authentication and source address verification, to ensure protocol security.
Reliability Measures	RIP uses function graceful restart (GR) to enhance reliability of the protocol.
Multiple Instances	RIP supports multiple instances and VPN applications.

3.3.1 RIPv1 and RIPv2

Two RIP versions are available: RIPv1 and RIPv2.

Working Principle

RIPv1

RIPv1 packets are broadcast. The broadcast address is 255.255.255.255, and the UDP port ID is 520. RIPv1 cannot identify the subnet mask, and supports only classful routes.

RIPv2

RIPv2 packets are multicast. The multicast address is 224.0.0.9, and the UDP port ID is 520. RIPv2 can identify the subnet mask, and supports classless routes, summarized route, and supernetting routes. RIPv2 supports plain text authentication and message digest 5 (MD5) authentication.

Related Configuration

Enabling the RIP Process

The RIP process is disabled by default.

Run the **router rip** command to enable the RIP process.

You must enable the RIP process on a device; otherwise, all functions related to RIP cannot take effect.

Running RIP on an Interface

By default, RIP does not run on an interface.

Run the **network** command to define an address range. RIP runs on interfaces that belong to this address range.

After RIP runs on an interface, RIP packets can be exchanged on the interface and RIP can learn routes to the network segments directly connected to the device.

Defining the RIP Version

By default, an interface receives RIPv1 and RIPv2 packets, and sends RIPv1 packets.

Run the **version** command to define the version of RIP packets sent or received on all interfaces.

Run the **ip rip send version** command to define the version of RIP packets sent on an interface.

Run the **ip rip receive version** command to define the version of RIP packets received on an interface.

If the versions of RIP running on adjacent routers are different, the RIPv1-enabled router will learn incorrect routes.

Preventing an Interface from Sending or Receiving Packets

By default, a RIP-enabled interface is allowed to send and receive RIP packets.

Run the **no ip rip receive enable** command to prevent an interface from receiving RIP packets.

Run the **no ip rip send enable** command to prevent an interface from sending RIP packets.

Run the **passive-interface** command to prevent an interface from sending broadcast or multicast RIP packets.

Configuring the Mode for Sending RIP Packets

By default, broadcast RIPv1 packets and multicast RIPv2 are sent.

Run the **ip rip v2-broadcast** command to send broadcast RIPv2 packets on an interface.

Run the **neighbor** command to send unicast RIP packets to a specified neighbor router.

3.3.2 Exchanging Routing Information

Compared with static routing, the dynamic routing protocol has a significant advantage, that is, by exchanging routing information, devices can automatically obtain routes to a remote network and update the routes in real time.

Working Principle

Initialization

After RIP is enabled on a router, the router sends a request packet to its neighbor router, requesting for all routing information, that is, the routing table. After receiving the request message, the neighbor router returns a response packet containing the local routing table. After receiving the response packet, the router updates the local routing table, and sends an update packet to the neighbor router, informing the neighbor router of the route update information. After receiving the update packet, the neighbor router updates the local routing table, and sends the update packet to other adjacent routers. After a series of updates, all routers can obtain and retain the latest routing information.

Periodical Update

By default, periodical update is enabled for RIP. Adjacent routers exchange complete routing information with each other every 30s (update timer), that is, the entire routing table is sent to neighbor routers. One update packet contains at most 25 routes. Therefore, a lot of update packets may be required to send the entire routing table. You can set the sending delay between update packets to avoid loss of routing information.

For every non-local route, if the route is not updated within 180s (invalid timer), the metric of the route is changed to 16 (unreachable). If the route is still not updated in the next 120s (flush timer), the route is deleted from the routing table.

Triggered Updates

After the triggered updates function is enabled, periodical update is automatically disabled. When routing information changes on a router, the router immediately sends routes related to the change (instead of the complete routing table) to the neighbor router, and use the acknowledgment and retransmission mechanisms to ensure that the neighbor router receives the routes successfully. Compared with periodical update, triggered updates help reduce flooding and accelerates route convergence.

Events that can trigger update include router startup, interface status change, changes in routing information (such as the metric), and reception of a request packet.

Route Summarization

When sending routing information to a neighbor router, the RIP-enabled router summarizes subnet routes that belong to the same classful network into a route, and sends the route to the neighbor router. For example, summarize 80.1.1.0/24 (metric=2) and 80.1.2.0/24 (metric=3) into 80.0.0.0/8 (metric=2), and set the metric of the summarized route to the optimum metric.

Only RIPv2 supports route summarization. Route summarization can reduce the size of the routing table and improve the efficiency of routing information exchange.

Supernetting Route

If the subnet mask length of a route is smaller than the natural mask length, this route is called supernetting route. For example, in the 80.0.0.0/6 route, as 80.0.0.0 is a Class A network address and the natural mask is 8 bits, 80.0.0.0/6 route is a supernetting route.

Only RIPv2 supports supernetting routes.

Default Route

In the routing table, a route to the destination network 0.0.0.0/0 is called default route.

The default route can be learned from a neighbor router, or sent to a neighbor router.

Route Redistribution

For RIP, other types of routes (such as direct routes, static routes, and routes of other routing protocols) are called external routes.

External routes (excluding the default route) can be redistributed to RIP and advertised to neighbors.

Route Filtering

Filtering conditions can be configured to limit the routing information exchanged between adjacent routers. Only the routing information that meets filtering conditions can be sent or received.

Related Configuration

Sending Delay Between Update Packets

By default, the update packets are sent continuously without any delay.
Run the **output-delay** command to set the sending delay between update packets.

RIP Timers

By default, the update timer is 30s, the invalid timer is 180s, and the flush timer is 120s.

Run the **timers basic** command to modify durations of the RIP timers.

Increasing the duration of the flush timer can reduce the route flapping. Decreasing the duration of the flush timer helps accelerate route convergence.

The durations of RIP timers must be consistent on adjacent routers. Unless otherwise required, you are advised not to modify the RIP timers.

Triggered Updates

By default, periodical update is enabled.

Run the **ip rip triggered** command to enable triggered updates on the interface and disable periodical update.

Run the **ip rip triggered retransmit-timer** command to modify the retransmission interval of update packets. The default value is 5s.

Run the **ip rip triggered retransmit-count** command to modify the maximum retransmission times of update packets. The default value is 36.

Route Summarization

By default, route summarization is automatically enabled if an interface is allowed to send RIPv2 packets.

Run the **no auto-summary** command to disable route summarization.

Run the **ip rip summary-address** command to configure route summarization on an interface.

Supernetting Route

By default, supernetting routes can be sent if an interface is allowed to send RIPv2 packets.

Run the **no ip rip send supernet-routes** command to prevent the sending of supernetting routes.

Default Route

Run the **ip rip default-information** command to advertise the default route to neighbors on an interface.

Run the **default-information originate** command to advertise the default route to neighbors from all interfaces.

Route Redistribution

Run the **redistribute** command to redistribute external routes (excluding the default route) to RIP and advertise them to neighbors.

Route Filtering

Run the **distribute-list out** command to set filtering rules to limit the routing information sent by the device.

Run the **distribute-list in** command to set filtering rules to limit the routing information received by the device.

3.3.3 Routing Algorithm

RIP is a protocol based on the distance-vector algorithm. It uses the vector addition method to compute the routing information.

Working Principle

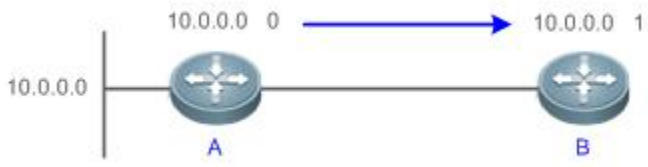
Distance-Vector Algorithm

RIP is a protocol based on the distance-vector algorithm. The distance-vector algorithm treats a route as a vector that consists of the destination network and distance (metric). The router obtains a route from its neighbor and adds the distance vector from itself to the neighbor to the route to form its own route.

RIP uses the hop count to evaluate the distance (metric) to the destination network. By default, the hop count from a router to its directly connected network is 0, the hop count from a router to a network that can be reached through the router is 1, and so on. That is, the metric is equal to the number of routers from the local network to the destination network. To restrict the convergence time, RIP stipulates that the metric must be an integer between 0 and 15. If the metric is equal to or greater than 16, the destination network or host is unreachable. For this reason, RIP cannot be applied on a large-scale network.

As shown in Figure 2- , Router A is connected to the network 10.0.0.0. Router B obtains the route (10.0.0.0,0) from Router A and adds the metric 1 to the route to obtain its own route ((10.0.0.0,1), and the next hop points to Router A.

Figure 2- 2

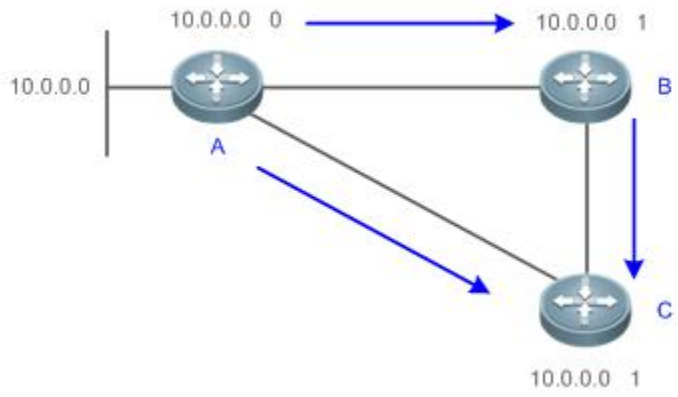


Selecting the Optimum Route

RIP selects an optimum route based on the following principle: If multiple routes to the same destination network is available, a router preferentially selects the route with the smallest metric.

As shown in Figure 2- , Router A is connected to the network 10.0.0.0. Router C obtains the route (10.0.0.0,0) from Router A and the route (10.0.0.0,1) from Router B. Router C will select the route that is obtained from Router A and add metric 1 to this route to form its own route (10.0.0.0,1), and the next hop points to Router A.

Figure 2- 3



When routes coming from different sources exist on a router, the route with the smallest distance is preferentially selected.

Route Source	Default Distance
Directly-connected network	0
Static route	1
OSPF route	110
RIP route	120
Unreachable route	255

Related Configuration

Modifying the Distance

By default, the distance of a RIP route is 120.

Run the **distance** command to modify the distance of a RIP route.

Modifying the Metric

For a RIP route that is proactively discovered by a device, the default metric is equal to the number of hops from the local network to the destination network. For a RIP router that is manually configured (default route or redistributed route), the default metric is 1.

Run the **offset-list in** command to increase the metric of a received RIP route.

Run the **offset-list out** command to increase the metric of a sent RIP route.

Run the **default-metric** command to modify the default metric of a redistributed route.

Run the **redistribute** command to modify the metric of a route when the route is redistributed.

Run the **default-information originate** command to modify the metric of a default route when the default route is introduced.

Run the **ip rip default-information** command to modify the metric of a default route when the default route is created.

3.3.4 Avoiding Route Loops

RIP uses functions, such as split horizon and poison reverse, to avoid route loops.

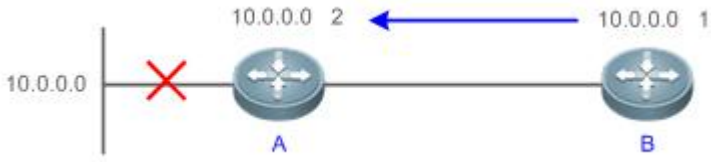
Working Principle

Route Loop

A RIP route loop occurs due to inherent defects of the distance-vector algorithm.

As shown in Figure 2- , Router A is connected to the network 10.0.0.0, and sends an update packet every 30s. Router B receives the route 10.0.0.0 from Router A every 30s. If Router A is disconnected from 10.0.0.0, the route to 10.0.0.0 will be deleted from the routing table on Router A. Next time, the update packet sent by Router A no longer contains this route. As Router B does not receive an update packet related to 10.0.0.0, Router B determines that the route to 10.0.0.0 is valid within 180s and uses the Update packet to send this route to Router A. As the route to 10.0.0.0 does not exist on Router A, the route learned from Router B is added to the routing table. Router B determines that data can reach 10.0.0.0 through Router A, and Router A determines that data can reach 10.0.0.0 through Router B. In this way, a route loop is formed.

Figure 2- 4

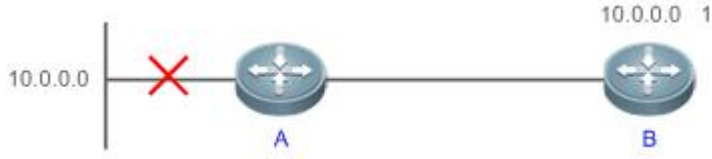


Split Horizon

Split horizon can prevent route loops. After split horizon is enabled on an interface, a route received on this interface will not be sent out from this interface.

As shown in Figure 2- , after split horizon is enabled on the interface between Router A and Router B, Router B will not send the route 10.0.0.0 back to Router A. Router B will learn 180s later that 10.0.0.0 is not reachable.

Figure 2- 5



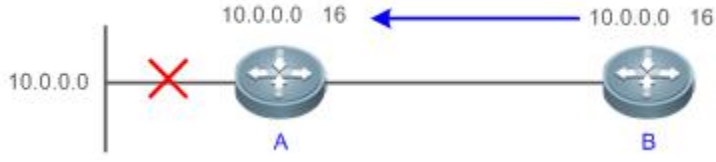
Poison Reverse

Poison reverse can also prevent route loops. Compared with slit horizon, poison reverse is more reliable, but brings more protocol packets, which makes network congestion more severe.

After poison reverse is enabled on an interface, a route received from this interface will be sent out from this interface again, but the metric of this router will be changed to 16 (unreachable).

As shown in Figure 2- , after learning the route 10.0.0.0 from Router A, Router B sets the metric of this route to 16 and sends the route back to Router A. After this route becomes invalid, Router B advertises the route 10.0.0.0 (metric = 16) to Router A to accelerate the process of deleting the route from the routing table.

Figure 2- 6



Related Configuration

Split Horizon

By default, split horizon is enabled.

Run the **no ip rip split-horizon** command to disable split horizon.

Poison Reverse

By default, poison reverse is disabled.

Run the **ip rip split-horizon poisoned-reverse** command to enable poison reverse. (After poison reverse is enabled, split horizon is automatically disabled.)

3.3.5 Security Measures

RIP uses functions, such as authentication and source address verification, to ensure protocol security.

Working Principle

Authentication

RIPv2 supports authentication, but RIPv1 does not.

After authentication is enabled on an interface, the routing information cannot be exchanged between adjacent devices if authentication fails. The authentication function is used to prevent unauthorized devices from accessing the RIP routing domain.

RIPv2 supports plain text authentication and MD5 authentication.

Source Address Verification

When a RIP-enabled device receives an Update packet, it checks whether the source IP address in the packet and the IP address of the inbound interface are in the same network segment. If not, the device drops the packet. Source address verification is used to ensure that RIP routing information is exchanged only between adjacent routing devices.

- On an unnumbered IP interface, source address verification is not performed (not configurable).
- If the triggered updates function is enabled, source address verification is automatically enabled (not configurable).
- If split horizon is disabled, source address verification is automatically enabled (not configurable).

Related Configuration

Authentication

By default, authentication is disabled.

Run the **ip rip authentication mode text** command to enable plain text authentication on an interface.

Run the **ip rip authentication mode md5** command to enable MD5 authentication on an interface.

Run the **ip rip authentication text-password** command to set the password for plain text authentication on an interface.

Run the **ip rip authentication key-chain** command to reference the key in the configured key chain as the authentication key on an interface.

Source Address Verification

By default, source address verification is enabled.

Run the **no validate-update-source** command to disable source address verification.

3.3.6 Reliability Measures

RIP uses GR function to enhance reliability of the protocol.

Working Principle

GR

GR ensures uninterrupted data transmission when the protocol is restarted. If RIP is restarted on a GR-enabled device, the forwarding table before restart will be retained and a request packet will be sent to the neighbor so that the route can be learned again. During the GR period, RIP completes re-convergence of the route. After the GR period expires, RIP updates the forwarding entry and advertises the routing table to the neighbor.

Related Configuration

GR

By default, GR is disabled.

Run the **graceful-restart** command to enable the GR function.

3.4 Configuration

Configuration	Description and Command	
Configuring RIP Basic Functions	(Mandatory) It is used to build a RIP routing domain.	
	router rip	Enables a RIP routing process and enters routing process configuration mode.
	network	Runs RIP on interfaces in the specified address range.
	version	Defines the RIP version.
	ip rip split-horizon	Enables split horizon or poison reverse on an interface.
	passive-interface	Configures a passive interface.
Controlling Interaction of RIP Packets	(Optional) This configuration is required if you wish to change the default mechanism for sending or receiving RIP packets.	
	neighbor	Sends unicast RIP packets to a specified neighbor.
	ip rip v2-broadcast	Sends broadcast RIPv2 packets on an interface.
	ip rip receive enable	Allows the interface to receive RIP packets.
	ip rip send enable	Allows the interface to send RIP packets.
	ip rip send version	Defines the version of RIP packets sent on an interface.
	ip rip receive version	Defines the version of RIP packets received on an interface.
Enabling Triggered Updates	Optional.	
	ip rip triggered	Enables triggered updates on an interface.
Enabling Source Address Verification	Optional.	
	validate-update-source	Enables source address verification.

Configuration	Description and Command	
Enabling Authentication	(Optional) Only RIPv2 supports authentication.	
	ip rip authentication mode	Enables authentication and sets the authentication mode on an interface.
	ip rip authentication text-password	Configures the password for plain text authentication on an interface.
	ip rip authentication key-chain	Configures the authentication key chain on an interface.
Enabling Route Summarization	(Optional) Only RIPv2 supports route summarization.	
	auto-summary	Enables automatic summarization of RIP routes.
	ip rip summary-address	Configures route summarization on an interface.
Enabling Supernetting Routes	(Optional) Only RIPv2 supports supernetting routes.	
	ip rip send supernet-routes	Enables advertisement of RIP supernetting routes on an interface
Advertising the Default Route or External Routes	Optional.	
	ip rip default-information	Advertises the default route to neighbors on an interface.
	default-information originate	Advertises the default route to neighbors.
	redistribute	Redistributes routes and advertises external routes to neighbors.
Setting Route Filtering Rules	Optional.	
	distribute-list in	Filters the received RIP routing information.
	distribute-list out	Filters the sent RIP routing information.
Modifying Route Selection Parameters	Optional.	
	distance	Modifies the administrative distance (AD) of a RIP route.
	offset-list	Increases the metric of a received or sent RIP route.
	default-metric	Configures the default metric of an external route redistributed to RIP.
Modifying Timers	Optional.	
	timers basic	Modifies the update timer, invalid timer, and flush timer.
	output-delay	Sets the sending delay between RIP route update packets.
Enabling GR	Optional.	
	graceful-restart	Configures the GR restarter capability.

3.4.1 Configuring RIP Basic Functions

Configuration Effect

- Build a RIP routing domain on the network.
- Routers in the domain obtain routes to a remote network through RIP.

Notes

- IPv4 addresses must be configured.
- IPv4 unicast routes must be enabled.

Configuration Steps

Enabling a RIP Routing Process

- Mandatory.
- Unless otherwise required, this configuration must be performed on every router in the RIP routing domain.

Associating with the Local Network

- Mandatory.
- Unless otherwise required, this configuration must be performed on every router in the RIP routing domain.
- Unless otherwise required, the local network associated with RIP should cover network segments of all L3 interfaces.

Defining the RIP Version

- If RIPv2 functions (such as the variable length subnet mask and authentication) are required, enable the RIPv2.
- Unless otherwise required, you must define the same RIP version on every router.

Enabling Split Horizon or Poison Reverse

- By default, split horizon is enabled and poison reverse is disabled.
- Unless otherwise required, enable split horizon on every interface connected to the broadcast network, such as the Ethernet. (Retain the default setting.)
- Unless otherwise required, enable split horizon on every interface connected to the point-to-point (P2P) network, such as the PPP and HDLC. (Retain the default setting.)
- It is recommended that split horizon and poison reverse be disabled on an interface connected to a non-broadcast multi-access (NBMA) network, such as FR and X.25; otherwise, some devices may fail to learn the complete routing information.
- If the secondary IP address is configured for an interface connected to a non-broadcast, it is recommended that split horizon and poison reverse be disabled.

Configuring a Passive Interface

- If you want to suppress Update packets on a RIP interface, configure the interface as a passive interface.
- Use the passive interface to set the boundary of the RIP routing domain. The network segment of the passive interface belongs to the RIP routing domain, but RIP packets cannot sent over the passive interface.
- If RIP routes need to be exchanged on an interface (such as the router interconnect interface) in the RIP routing domain, this interface cannot be configured as a passive interface.

Verification

- Check the routing table on a router to verify that the route to a remote network can be obtained through RIP.

Related Commands

Enabling a RIP Routing Process

Command Syntax	**router rip**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	This command is used to create a RIP routing process and enter routing process configuration mode.

Associating with the Local Network

Command Syntax	**network** *network-number* [*wildcard*]
Parameter Description	*network-number*: Indicates the number of a network. *wildcard*: Defines the IP address comparison bit. **0** indicates accurate matching, and **1** indicates that no comparison is performed.
Command Mode	Routing process configuration mode
Configuration Usage	RIP can run and learn direct routes and RIP packets can be exchanged only on an interface covered by **network**. If **network** 0.0.0.0 255.255.255.255 is configured, all interfaces are covered. If *wildcard* is not configured, the classful address range is used by default, that is, the interfaces whose addresses fall into the classful address range participate in RIP operations.

Defining the RIP Version

Command Syntax	**version** { **1** | **2** }
Parameter Description	**1**: Indicates RIPv1. **2**: Indicates RIPv2.
Command Mode	Global configuration mode
Configuration Usage	This command takes effect on the entire router. You can run this command to define the version of RIP packets sent or received on all interfaces.

Enabling Split Horizon

Command Syntax	**ip rip split-horizon** [**poisoned-reverse**]
Parameter Description	**poisoned-reverse**: Indicates poison reverse.
Command Mode	Interface configuration mode

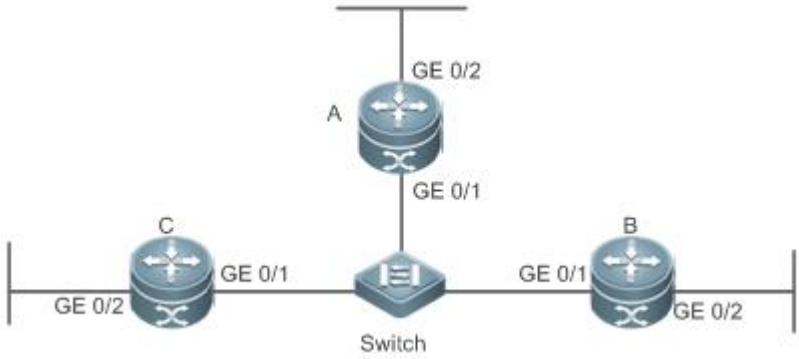
Configuration Usage	After poison reverse is enabled, split horizon is automatically disabled.

Configuring a Passive Interface

Command Syntax	**passive-interface** { **default** | *interface-type interface-num* }
Parameter Description	**default:** Indicates all interfaces. ***interface-type interface-num***: Specifies an interface.
Command Mode	Routing process configuration mode
Configuration Usage	First, run the **passive-interface default** command to configure all interfaces as passive interfaces. Then, run the **no passive-interface** *interface-type interface-num* command to cancel the interfaces used for interconnection between routers in the domain.

Configuration Example

Building a RIP Routing Domain

Scenario Figure 2- 7	 **Remarks**: The interface IP addresses are as follows: A: GE0/1 110.11.2.1/24 GE0/2 155.10.1.1/24 B: GE0/1 110.11.2.2/24 GE0/2 196.38.165.1/24 C: GE0/1 110.11.2.3/24 GE0/2 117.102.0.1/16
Configuration Steps	● Configure the interface IP addresses on all routers. ● Configure the RIP basic functions on all routers.
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 110.11.2.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# exit A(config)# interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)# ip address 155.10.1.1 255.255.255.0 A(config)# router rip A(config-router)# version 2 A(config-router)# network 0.0.0.0 255.255.255.255

	A(config-router)# passive-interface default A(config-router)# no passive-interface GigabitEthernet 0/1
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip address 110.11.2.2 255.255.255.0 B(config-if-GigabitEthernet 0/1)# exit B(config)# interface GigabitEthernet 0/2 B(config-if-GigabitEthernet 0/2)# ip address 196.38.165.1 255.255.255.0 B(config-if-GigabitEthernet 0/2)# exit B(config)# router rip B(config-router)# version 2 B(config-router)# network 0.0.0.0 255.255.255.255 B(config-router)# passive-interface default B(config-router)# no passive-interface GigabitEthernet 0/1
C	C# configure terminal C(config)# interface GigabitEthernet 0/1 C(config-if-GigabitEthernet 0/1)# ip address 110.11.2.3 255.255.255.0 C(config-if-GigabitEthernet 0/1)# exit C(config)# interface GigabitEthernet 0/2 C(config-if-GigabitEthernet 0/2)# ip address 117.102.0.1 255.255.0.0 C(config-if-GigabitEthernet 0/2)# exit C(config)# router rip C(config-router)# version 2 C(config-router)#no auto-summary C(config-router)# network 0.0.0.0 255.255.255.255 C(config-router)# passive-interface default C(config-router)# no passive-interface GigabitEthernet 0/1
Verification	Check the routing tables on Router A, Router B, and Router C. Verify that RIP learns the routes to remote networks (contents marked in blue).
A	A# show ip route Codes: C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area

	N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default Gateway of last resort is no set C 110.11.2.0/24 is directly connected, GigabitEthernet 0/1 C 110.11.2.1/32 is local host. R 117.0.0.0/8 [120/1] via 110.11.2.2, 00:00:47, GigabitEthernet 0/1 C 155.10.1.0/24 is directly connected, GigabitEthernet 0/2 C 155.10.1.1/32 is local host. C 192.168.217.0/24 is directly connected, VLAN 1 C 192.168.217.233/32 is local host. R 196.38.165.0/24 [120/1] via 110.11.2.3, 00:19:18, GigabitEthernet 0/1
B	B# show ip route Codes: C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default Gateway of last resort is no set C 110.11.2.0/24 is directly connected, GigabitEthernet 0/1 C 110.11.2.2/32 is local host. R 155.10.0.0/16 [120/1] via 110.11.2.1, 00:15:21, GigabitEthernet 0/1 C 196.38.165.0/24 is directly connected, GigabitEthernet 0/2 C 196.38.165.1/32 is local host. R 117.0.0.0/8 [120/1] via 110.11.2.2, 00:00:47, GigabitEthernet 0/1
C	C# show ip route Codes: C - connected, S - static, R - RIP, B - BGP

	O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default Gateway of last resort is no set C 110.11.2.0/24 is directly connected, GigabitEthernet 0/1 C 110.11.2.3/32 is local host. C 117.102.0.0/16 is directly connected, GigabitEthernet 0/2 C 117.102.0.1/32 is local host. R 155.10.0.0/16 [120/1] via 110.11.2.1, 00:20:55, GigabitEthernet 0/1 R 196.38.165.0/24 [120/1] via 110.11.2.3, 00:19:18, GigabitEthernet 0/1

Common Errors

- The IPv4 address is not configured on an interface.
- The RIP version is not defined on a device, or the RIP version on the device is different from that on other routers.
- The address range configured by the **network** command does not cover a specific interface.
- The **wildcard** parameter in the **network** command is not correctly configured. **0** indicates accurate matching, and **1** indicates that no comparison is performed.
- The interface used for interconnection between devices is configured as a passive interface.

3.4.2 Controlling Interaction of RIP Packets

Configuration Effect

Change the default running mechanism of RIP through configuration and manually control the interaction mode of RIP packets, including:

- Allowing or prohibiting the sending of unicast RIP packets to a specified neighbor on an interface
- Allowing or prohibiting the sending of unicast RIPv2 packets instead of broadcast packets to a specified neighbor on an interface
- Allowing or prohibiting the receiving of RIP packets on an interface
- Allowing or prohibiting the sending of RIP packets on an interface
- Allowing or prohibiting the receiving of RIP packets of a specified version on an interface
- Allowing or prohibiting the sending of RIP packets of a specified version on an interface

Notes

- The RIP basic functions must be configured.

- On an interface connecting to a neighbor device, the configured version of sent RIP packets must be the same as the version of received RIP packets.

Configuration Steps

Sending Unicast RIP Route Update Packets to a Specified Neighbor

- Configure this function if you wish that only some of devices connected to an interface can receive the updated routing information.
- By default, RIPv1 uses the IP broadcast address (255.255.255.255) to advertise the routing information, whereas RIPv2 uses the multicast address (224.0.0.9) to advertise the routing information. If you do not wish all devices on the broadcast network or NBMA network to receive routing information, configure the related interface as the passive interface and specify the neighbors that can receive the routing information. This command does not affect the receiving of RIP packets. RIPv2 packets are broadcast on an interface.
- Unless otherwise required, this function must be enabled on a router that sends the unicast Update packets.

Broadcasting RIPv2 Packets on an Interface

- This function must be configured if the neighbor router does not support the receiving of multicast RIPv2 packets.
- Unless otherwise required, this function must be configured on every router interface that broadcasts RIPv2 packets.

Allowing an Interface to Receive RIP Packets

- This function is enabled by default, and must be disabled if an interface is not allowed to receive RIP packets.
- Unless otherwise required, this function must be configured on every router interface that is not allowed to receive RIP packets.

Allowing an Interface to Send RIP Packets

- This function is enabled by default, and must be disabled if an interface is not allowed to send RIP packets.
- Unless otherwise required, this function must be configured on every router interface that is not allowed to send RIP packets.

Allowing an Interface to Send RIP Packets of a Specified Version

- This function must be configured if the version of RIP packets that can be sent on an interface is required to be different from the global configuration.
- Unless otherwise required, this function must be configured on every router interface that is allowed to send RIP packets of a specified version.

Allowing an Interface to Receive RIP Packets of a Specified Version

- This function must be configured if the version of RIP packets that can be received on an interface is required to be different from the global configuration.
- Unless otherwise required, this function must be configured on every router interface that is allowed to receive RIP packets of a specified version.

Verification

Run the **debug ip rip packet** command to verify the packet sending result and packet type.

Related Commands

Sending Unicast RIP Route Update Packets to a Specified Neighbor

Command Syntax	**neighbor** *ip-address*
Parameter Description	*ip-address:* Indicates the IP address of the neighbor. It should be the address of the network directly connected to the local device.
Command Mode	Routing process configuration mode
Configuration Usage	Generally, you can first run the **passive-interface** command in routing process configuration mode to configure the related interface as a passive interface, and then specify the neighbors that can receive the routing information. This command does not affect the receiving of RIP packets. After an interface is configured as a passive interface, the interface does not send the request packets even after the device is restarted.

Broadcasting RIPv2 Packets on an Interface

Command Syntax	**ip rip v2-broadcast**
Parameter Description	N/A
Command Mode	Interface configuration mode
Configuration Usage	The default behavior is determined by the configuration of the **version** command. The configuration result of this command can overwrite the default configuration of the **version** command. This command affects the behavior of sending RIP packets on the current interface, and the interface is allowed to send RIPv1 and RIPv2 packets simultaneously. If this command does not contain any parameter, the behavior of receiving RIP packets is determined by the configuration of the **version** command.

Allowing an Interface to Receive RIP Packets

Command Syntax	**ip rip receive enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Configuration Usage	To prohibit the receiving of RIP packets on an interface, use the **no** form of this command. This command takes effect only on the current interface. You can use the **default** form of the command to restore the default setting, that is, allowing the interface to receive RIP packets.

Allowing an Interface to Send RIP Packets

Command Syntax	**ip rip send enable**
Parameter Description	N/A
Command Mode	Interface configuration mode

Configuration Usage	To prohibit the sending of RIP packets on an interface, use the **no** form of this command in interface configuration mode. This command takes effect only on the current interface. You can use the **default** form of the command to restore the default setting, that is, allowing the interface to send RIP packets.

Allowing an Interface to Send RIP Packets of a Specified Version

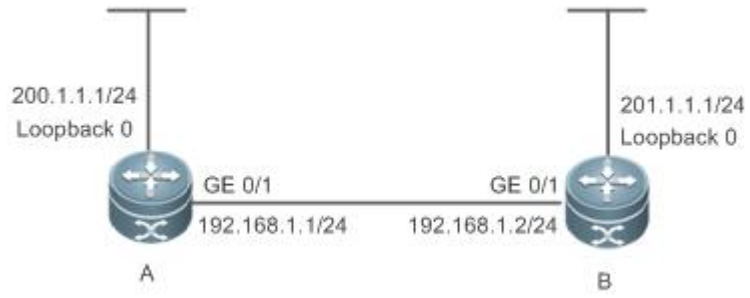
Command Syntax	**ip rip send version** [**1**] [**2**]
Parameter Description	**1**: Indicates that only RIPv1 packets are sent. **2**: Indicates that only RIPv2 packets are sent.
Command Mode	Interface configuration mode
Configuration Usage	The default behavior is determined by the configuration of the **version** command. The configuration result of this command can overwrite the default configuration of the **version** command. This command affects the behavior of sending RIP packets on the current interface, and the interface is allowed to send RIPv1 and RIPv2 packets simultaneously. If this command does not contain any parameter, the behavior of receiving RIP packets is determined by the configuration of the **version** command.

Allowing an Interface to Receive RIP Packets of a Specified Version

Command Syntax	**ip rip receive version** [**1**] [**2**]
Parameter Description	**1**: Indicates that only RIPv1 packets are received. **2**: Indicates that only RIPv2 packets are received.
Command Mode	Interface configuration mode
Configuration Usage	The default behavior is determined by the configuration of the **version** command. The configuration result of this command can overwrite the default configuration of the **version** command. This command affects the behavior of receiving RIP packets on the current interface, and the interface is allowed to receive RIPv1 and RIPv2 packets simultaneously. If this command does not contain any parameter, the behavior of receiving RIP packets is determined by the configuration of the **version** command.

Configuration Example

Prohibiting an Interface from Sending RIP Packets

Scenario Figure 2-8	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Prohibit the sending of RIP packets on an interface of Router A.

A	A# configure terminal A(config)# interface GigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# no ip rip send enable
Verification	Run the **debug ip rip packet send** command on Router A, and verify that packets cannot be sent.
A	A# debug ip rip packet recv *Nov 4 08:19:31: %RIP-7-DEBUG: [RIP] Prepare to send BROADCAST response... *Nov 4 08:19:31: %RIP-7-DEBUG: [RIP] Building update entries on GigabitEthernet 0/1 *Nov 4 08:19:31: %RIP-7-DEBUG: 117.0.0.0/8 via 0.0.0.0 metric 1 tag 0 *Nov 4 08:19:31: %RIP-7-DEBUG: [RIP] Interface GigabitEthernet 0/1 is disabled to send RIP packet!

Common Errors

A compatibility error occurs because the RIP version configured on the neighbor is different from that configured on the local device.

3.4.3 Enabling Triggered Updates

Configuration Effect

- Enable the RIP triggered updates function, after which RIP does not periodically send the route update packets.

Notes

- The RIP basic functions must be configured.
- It is recommended that split horizon with poisoned reverse be enabled; otherwise, invalid routing information may exist.
- This function cannot be enabled together with the function of correlating RIP with BFD.
- Ensure that the triggered updates function is enabled on every router on the same link; otherwise, the routing information cannot be exchanged properly.

Configuration Steps

Enabling Triggered Updates

- This function must be enabled if demand circuits are configured on the WAN interface.
- The triggered updates function can be enabled in either of the following cases: (1) The interface has only one neighbor; (2) The interface has multiple neighbors but the device interacts with these neighbors in unicast mode.
- It is recommended that triggered updates be enabled on a WAN interface (running the PPP, Frame Relay, or X.25 link layer protocol) to meet the requirements of demand circuits.
- If the triggered updates function is enabled on an interface, source address verification is performed no matter whether the source address verification function is enabled by the **validate-update-source** command.
- Unless otherwise required, triggered updates must be enabled on demand circuits of every router.

Verification

When the RIP triggered updates function is enabled, RIP cannot periodically send the route update packets. RIP sends the route update packets to the WAN interface only in one of the following cases:

- A route request packet is received.
- The RIP routing information changes.
- The interface state changes.
- The router is started.

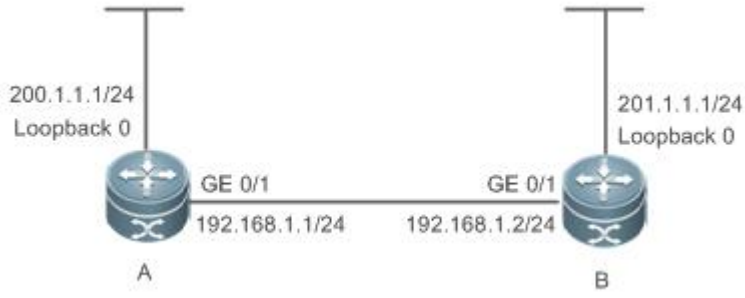
Related Commands

Enabling Triggered Updates

Command Syntax	**ip rip triggered** { **retransmit-timer** *timer* / **retransmit-count** *count* }
Parameter Description	**retransmit-timer** *timer*: Configures the interval at which the update request or update response packet is retransmitted. The default value is 5s. The value ranges from 1 to 3,600. **retransmit-count** *count*: Configures the maximum retransmission times of the update request or update response packet. The default value is 36. The value ranges from 1 to 3,600.
Command Mode	Interface configuration mode
Configuration Usage	You can run the **ip rip triggered** command to enable the RIP triggering function. When this function is enabled, the RIP periodical update function is automatically disabled. Therefore, the acknowledgment and retransmission mechanisms must be used to ensure that the Update packets are successfully sent or received on the WAN. You can use the **retransmit-timer** and **retransmit-count** parameters to specify the retransmission interval and maximum retransmission times of the request and update packets.

Configuration Example

Enabling Triggered Updates

Scenario **Figure 2- 9**	
Configuration Steps	- Configure the interface IP addresses on all routers. (Omitted) - Configure the RIP basic functions on all routers. (Omitted) - On Router A, enable the RIP triggered updates function, and set the retransmission interval and maximum retransmission times of the request and update packets to 10s and 18, respectively.
A	A# configure terminal A(config)# interface GigabitEthernet 0/1

	A(config-if-GigabitEthernet 0/1)# encapsulation ppp A(config-if-GigabitEthernet 0/1)# ip rip triggered A(config-if-GigabitEthernet 0/1)# ip rip triggered retransmit-timer 10 A(config-if-GigabitEthernet 0/1)# ip rip triggered retransmit-count 18 A(config-if-GigabitEthernet 0/1)# ip rip split-horizon poisoned-reverse A(config)# router rip A(config-router)# network 192.168.1.0 A(config-router)# network 200.1.1.0
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# encapsulation ppp B(config-if-GigabitEthernet 0/1)# ip rip triggered B(config-if-GigabitEthernet 0/1)# ip rip split-horizon poisoned-reverse B(config)# router rip B(config-router)# network 192.168.1.0 B(config-router)# network 201.1.1.0
Verification	On Router A and Router B, check the RIP database and verify that the corresponding routes are permanent.
A	A# sho ip rip database 201.1.1.0/24 auto-summary 201.1.1.0/24 [1] via 192.168.12.2 GigabitEthernet 0/1 06:25 permanent
B	B# sho ip rip database 200.1.1.0/24 auto-summary 200.1.1.0/24 [1] via 192.168.12.1 GigabitEthernet 0/1 06:25 permanent

Common Errors

- The triggered updates function is enabled when the RIP configurations at both ends of the link are consistent.
- The triggered updates function is not enabled on all routers on the same link.

3.4.4 Enabling Source Address Verification

Configuration Effect

- The source address of the received RIP route update packet is verified.

Notes

- The RIP basic functions must be configured.

Configuration Steps

Enabling Source Address Verification

- This function is enabled by default, and must be disabled when source address verification is not required.
- After split horizon is disabled on an interface, the RIP routing process will perform source address verification on the Update packet no matter whether the **validate-update-source** command is executed in routing process configuration mode.
- For an IP unnumbered interface, the RIP routing process does not perform source address verification on the Update packet no matter whether the **validate-update-source** command is executed in routing process configuration mode.
- Unless otherwise required, this function must be disabled on every router that does not requires source address verification.

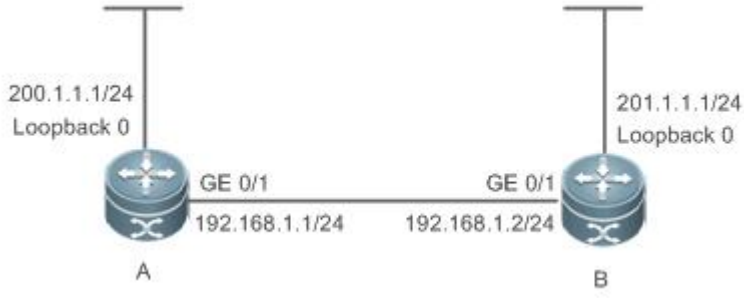
Verification

Only the route update packets coming from the same IP subnet neighbor are received.

Related Commands

Command Syntax	**validate-update-source**
Parameter Description	N/A
Command Mode	Routing process configuration mode
Configuration Usage	Source address verification of the Update packet is enabled by default. After this function is enabled, the source address of the RIP route update packet is verified. The purpose is to ensure that the RIP routing process receives only the route update packets coming from the same IP subnet neighbor.

Configuration Example

Scenario Figure 2- 10	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Disable source address verification of Update packets on all routers.

A	A# configure terminal A(config)# router rip A(config-router)# no validate-update-source
B	B# configure terminal B(config)# router rip B(config-router)# no validate-update-source
Verification	● On Router A, check the routing table and verify that the entry 201.1.1.0/24 is loaded. ● On Router B, check the routing table and verify that the entry 200.1.1.0/24 is loaded.
A	A# show ip route rip R 201.1.1.0/24 [120/1] via 192.168.2.2, 00:06:11, GigabitEthernet 0/1
B	B# show ip route rip R 200.1.1.0/24 [120/1] via 192.168.1.1, 00:06:11, GigabitEthernet 0/1

3.4.5 Enabling Authentication

Configuration Effect

- Prevent learning unauthenticated and invalid routes and advertising valid routes to unauthorized devices, ensuring stability of the system and protecting the system against intrusions.

Notes

- The RIP basic functions must be configured.
- Only RIPv2 supports authentication of RIP packets, and RIPv1 does not.

Configuration Steps

Enabling Authentication and Specifying the Key Chain Used for RIP Authentication

- This configuration is mandatory if authentication must be enabled.
- If the key chain is already specified in the interface configuration, run the **key chain** command in global configuration mode to define the key chain; otherwise, authentication of RIP packets may fail.
- Unless otherwise required, this configuration must be performed on every router that requires authentication.

Defining the RIP Authentication Mode

- This configuration is mandatory if authentication must be enabled.
- The RIP authentication modes configured on all devices that need to directly exchange RIP routing information must be the same; otherwise, RIP packets may fail to be exchanged.
- If plain text authentication is used, but the key chain for plain text authentication is not configured or associated, authentication is not performed. Similarly, if MD5 authentication is used, but the key chain is not configured or associated, authentication is not performed.

- Unless otherwise required, this configuration must be performed on every router that requires authentication.

Enabling RIP Plain Text Authentication and Configuring the Key Chain

- This configuration is mandatory if authentication must be enabled.
- If RIP plain text authentication should be enabled, use this command to configure the key chain for plain text authentication. Alternatively, you can obtain the key chain for plain text authentication by associating the key chain. The key chain obtained using the second method takes precedence over that obtained using the first method.
- Unless otherwise required, this configuration must be performed on every router that requires authentication.

Verification

- RIP plain text authentication provides only limited security because the password transferred through the packet is visible.
- RIP MD5 authentication can provide higher security because the password transferred through the packet is encrypted using the MD5 algorithm.
- Routes can be learned properly if the correct authentication parameters are configured.
- Routes cannot be learned if the incorrect authentication parameters are configured.

Related Commands

Enabling Source Address Verification

Command Syntax	**ip rip authentication key-chain** *name-of-keychain*
Parameter Description	*name-of-keychain*: Specifies the name of the key chain used for RIP authentication.
Command Mode	Interface configuration mode
Configuration Usage	The specified key chain must be defined by the **key chain** command in global configuration mode in advance.

Defining the RIP Authentication Mode

Command Syntax	**ip rip authentication mode** { **text** | **md5** }
Parameter Description	**text:** Indicates that the RIP authentication mode is plain text authentication. **md5:** Indicates that the RIP authentication mode is MD5 authentication.
Command Mode	Interface configuration mode
Configuration Usage	For all devices that need to directly exchange the RIP routing information, the RIP authentication mode of these devices must be the same.

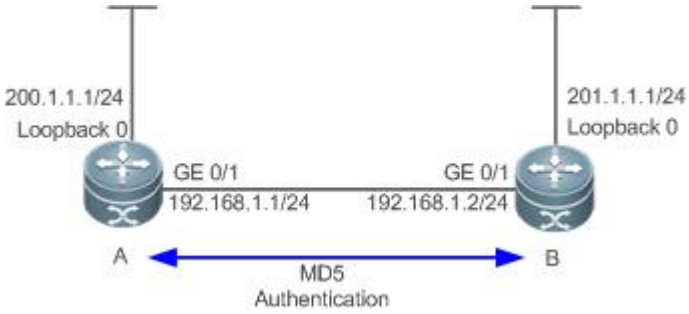
Enabling RIP Plain Text Authentication and Configuring the Key Chain

Command Syntax	**ip rip authentication text-password** [**0** | **7**] *password-string*
Parameter Description	**0**: Indicates that the key is displayed in plain text. **7**: Indicates that the key is displayed in cipher text.

	password-string: Indicates the key chain used for plain text authentication. The key chain is a string of 1 to 16 bytes.
Command Mode	Interface configuration mode
Configuration Usage	This commands takes effect only in plain text authentication mode.

Configuration Example

Configuring RIP Basic Functions and Enabling MD5 Authentication

Scenario **Figure 2- 11**	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Configure the authentication type and MD5 authentication key on all routers.
A	A# configure terminal A(config)# key chain hello A(config-keychain)# key 1 A(config-keychain-key)# key-string world A(config-keychain-key)# exit A(config-keychain)# exit A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip rip authentication mode md5 A(config-if-GigabitEthernet 0/1)# ip rip authentication key-chain hello
B	B# configure terminal B(config)# key chain hello B(config-keychain)# key 1 B(config-keychain-key)# key-string world B(config-keychain-key)# exit B(config-keychain)# exit B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip rip authentication mode md5 B(config-if-GigabitEthernet 0/1)# ip rip authentication key-chain hello

Verification	● On Router A, check the routing table and verify that the entry 201.1.1.0/24 is loaded. ● On Router B, check the routing table and verify that the entry 200.1.1.0/24 is loaded.
A	A# show ip route rip R 201.1.1.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1
B	A# show ip route rip R 200.1.1.0/24 [120/1] via 192.168.1.1, 00:06:11, GigabitEthernet 0/1

Common Errors

- The keys configured on routers that need to exchange RIP routing information are different.
- The authentication modes configured on routers that need to exchange RIP routing information are different.

3.4.6 Enabling Route Summarization

Configuration Effect

Reduce the size of the routing table, improve the routing efficiency, avoid route flapping to some extent, and improve scalability and effectiveness of the network.

- If a summarized route exists, subroutes included by the summarized route cannot be seen in the routing table, which greatly reduces the size of the routing table.
- Advertising a summarized route is more efficient than advertising individual routes because: (1) A summarized route is processed first when RIP looks through the database; (2) All subroutes are ignored when RIP looks through the database, which reduces the processing time required.

Notes

- The RIP basic functions must be configured.
- The range of supernetting routes is larger than that of the classful network. Therefore, the automatic route summarization function is invalid for supernetting routes.
- RIPv1 always performs automatic route summarization. If the detailed routes should be advertised, you must set the RIP version to RIPv2.

Configuration Steps

Enabling Automatic Route Summarization

- This function is enabled by default.
- To learn specific subnet routes instead of summarized network routes, you must disable automatic route summarization.
- You can disable automatic route summarization only in RIPv2. RIPv1 always performs automatic route summarization.

Configuring RIP Route Summarization on an Interface

- This function must be configured if it is required to summarize classful subnets.

- The **ip rip summary-address** command is used to summarize an address or a subnet under a specified interface. RIP automatically summarizes to the classful network boundary. Each classful subnet can be configured only in the **ip rip summary-address** command.
- The summary range configured in this command cannot be supernetting routes, that is, the configured subnet mask length cannot be smaller than the natural mask length of the network.
- Unless otherwise required, this configuration should be performed on a router that requires classful subnet summarization.

Verification

Verify that the routes are summarized in the routing table of the peer end.

Related Commands

Enabling Automatic Route Summarization

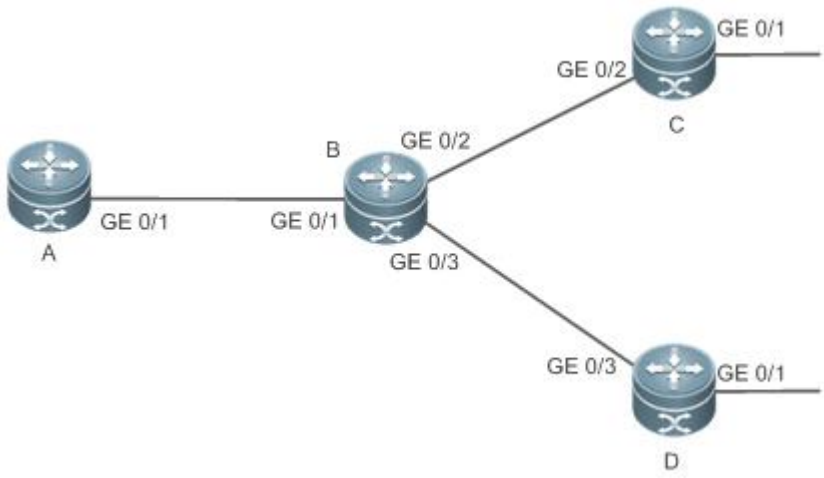
Command Syntax	**auto-summary**
Parameter Description	N/A
Command Mode	Routing process configuration mode
Configuration Usage	Route summarization is enabled by default for RIPv1 and RIPv2. You can disable automatic route summarization only in RIPv2. RIPv1 always performs automatic route summarization.

Configuring RIP Route Summarization on an Interface

Command Syntax	**ip rip summary-address** *ip-address ip-network-mask*
Parameter Description	*ip-address*: Indicates the IP address to be summarized. *ip-network-mask*: Indicates the subnet mask of the IP address to be summarized.
Command Mode	Interface configuration mode
Configuration Usage	This command is used to summarize an address or a subnet under a specified interface.

Configuration Example

Configuring Route Summarization

Scenario Figure 2- 12	 **Remarks**: The interface IP addresses are as follows: A: GE0/1 192.168.1.1 B: GE0/1 192.168.1.2 GE0/2 172.16.2.1 GE0/3 172.16.3.1 C: GE0/2 172.16.2.2 GE0/3 172.16.4.2 D: GE0/2 172.16.3.2 GE0/3 172.16.5.2
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Configure route summarization on Router B.
	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip rip summary-address 172.16.0.0 255.255.0.0 B(config)# router rip B(config-router)# version 2 B(config-router)# no auto-summary
Verification	Check the routing table on Router A, and verify that the entry 172.16.0.0/16 is generated.
	A# show ip route rip R 172.16.0.0/16 [120/2] via 192.168.1.2, 00:01:04, GigabitEthernet 0/1

Common Errors

- RIP basic functions are not configured or fail to be configured.

3.4.7 Enabling Supernetting Routes

Configuration Effect

- Allow RIP to send RIP supernetting routes on a specified interface.

Notes

- The RIP basic functions must be configured.

Configuration Steps

Enabling Supernetting Routes

- If a supernetting route is detected when a RIPv1-enabled router monitors the RIPv2 route response packets, the router will learn an incorrect route because RIPv1 ignores the subnet mask in the routing information of the packet. In this case, the **no** form of the command must be used on the RIPv2-enabled router to prohibit advertisement of supernetting routes on the related interface. This command takes effect only on the current interface.
- The command is effective only when RIPv2 packets are sent on the interface, and is used to control the sending of supernetting routes.

Verification

Verify that the peer router cannot learn the supernetting route.

Related Commands

Command Syntax	ip rip send supernet-routes
Parameter Description	N/A
Command Mode	Interface configuration mode
Configuration Usage	By default, an interface is allowed to send RIP supernetting routes.

Configuration Example

Disabling Supernetting Routes

Scenario Figure 2- 13	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Prohibit the sending of RIP supernetting routes on the GigabitEthernet 0/1 interface of Router B.

	B# configure terminal B(config)# ip route 207.0.0.0 255.0.0.0 Null 0 B(config)# ip route 208.1.1.0 255.255.255.0 Null 0 B(config)# router rip B(config-router)# redistribute static B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# no ip rip send supernet-routes
Verification	Check the routing table on Router A, and verify that Router A can learn only the non-supernetting route 208.1.1.0/24, but not the supernetting route 207.0.0.0/8.
	A#show ip route rip R 208.1.1.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1

3.4.8 Advertising the Default Route or External Routes

Configuration Effect

- In the RIP domain, introduce a unicast route of another AS so that the unicast routing service to this AS can be provided for users in the RIP domain.
- In the RIP domain, inject a default route to another AS so that the unicast routing service to this AS can be provided for users in the RIP domain.

Notes

- The RIP basic functions must be configured.
- Route redistribution cannot introduce default routes of other protocols to the RIP routing domain.

Configuration Steps

Advertising the Default Route to Neighbors

This function must be enabled if it is required to advertise the default route to neighbors.

By default, a default route is not generated, and the metric of the default route is 1.

If the RIP process can generate a default route using this command, RIP does not learn the default route advertised by the neighbor.

Unless otherwise required, this configuration should be performed on a router that needs to advertise the default route.

Advertising the Default Route to Neighbors on an Interface

This function must be enabled if it is required to advertise the default route to neighbors on a specified interface.

By default, a default route is not configured and the metric of the default route is 1.

After this command is configured on an interface, a default route is generated and advertised through this interface.

Unless otherwise required, this configuration should be performed on a router that needs to advertise the default route.

Redistributes Routes and Advertises External Routes to Neighbors

This function must be enabled if routes of other protocols need to be redistributed.

By default,

- If OSPF redistribution is configured, redistribute the routes of all sub-types of the OSPF process.
- In other cases, redistribute all external routes.
- The metric of a redistributed route is 1 by default.
- The route map is not associated by default.

During route redistribution, it is not necessary to convert the metric of one routing protocol to the metric of another routing protocol because different routing protocols use completely different metric measurement methods. RIP measures the metric based on the hop count, and OSPF measures the metric based on the bandwidth. Therefore, the computed metrics cannot be compared with each other. During route redistribution, however, it is necessary to configure a symbolic metric; otherwise, route redistribution fails.

Unless otherwise required, this configuration should be performed on a router that needs to redistribute routes.

Verification

- On a neighbor device, verify that a default route exists in the RIP routing table.
- On the local and neighbor devices, verify that external routes (routes to other ASs) exist in the RIP routing table.

Related Commands

Advertising the Default Route to Neighbors

Command Syntax	**default-information originate** [**always**] [**metric** *metric-value*] [**route-map** *map-name*]
Parameter Description	**always:** Enables RIP to generate a default route no matter whether the local router has a default route. **metric** *metric-value:* Indicates the initial metric of the default route. The value ranges from 1 to 15. **route-map** *map-name:* Indicates the associated route map name. By default, no route map is associated.
Command Mode	Routing process configuration mode
Configuration Usage	If a default route exists in the routing table of a router, RIP does not advertise the default route to external entities by default. You need to run the **default-information originate** command in routing process configuration mode to advertise the default route to neighbors. If the **always** parameter is selected, the RIP routing process advertises a default route to neighbors no matter the default route exists, but this default route is not displayed in the local routing table. To check whether the default route is generated, run the **show ip rip database** command to check the RIP routing information database. To further control the behavior of advertising the RIP default route, use the **route-map** parameter. For example, run the **set metric** rule to set the metric of the default route. You can use the **metric** parameter to set the metric of the advertised default value, but the priority of this configuration is lower than that of the set metric rule of the **route-map** parameter. If the **metric** parameter is not configured, the default route uses the default metric configured for RIP. You still need to run the **default-information originate** command to introduce the default route generated by **ip default-network** to RIP.

Advertising the Default Route to Neighbors on an Interface

Command Syntax	**ip rip default-information** { **only** | **originate** } [**metric** *metric-value*]
Parameter Description	**only**: Indicates that only the default route is advertised. **originate**: Indicates that the default route and other routes are advertised. **metric** *metric-value:* Indicates the metric of the default route. The value ranges from 1 to 15.
Command Mode	Interface configuration mode
Configuration Usage	If you configure the **ip rip default-information** command for the interface, and the **default-information originate** command for the RIP process, only the default route configured for the interface is advertised. So far as **ip rip default-information** is configured for one interface, RIP does not learn the default route advertised by the neighbor.

Redistributes Routes and Advertises External Routes to Neighbors

Command Syntax	**redistribute** {**connected** |**ospf** *process-id* | **static** } [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] [**metric** *metric-value*] [**route-map** *route-map-name*]
Parameter Description	**connected**: Indicates redistribution from direct routes. **ospf** *process-id*: Indicates redistribution from OSPF. *process-id* indicates the OSPF process ID. The value ranges from 1 to 65535. **static**: Indicates redistribution from static routes. **match**: Used only when OSPF routes are redistributed. Only the routes that match the filtering conditions are redistributed. **metric** *metric-value*: Sets the metric of the redistributed route. The value ranges from 1 to 16. **route-map** *route-map-name*: Sets the redistribution filtering rules.
Command Mode	Routing process configuration mode
Configuration Usage	If you configure redistribution of OSPF routes without specifying the **match** parameter, OSPF routes of all sub-types can be distributed by default. The latest setting of the **match** parameter is used as the initial **match** parameter. Only routes that match the sub-types can be redistributed. You can use the **no** form of the command to restore the default value of **match**. The configuration rules for the **no** form of the **redistribute** command are as follows: 1. If some parameters are specified in the **no** form of the command, default values of these parameters will be restored. 2. If no parameter is specified in the **no** form of the command, the entire command will be deleted.

Configuration Example

Redistributing Routes and Advertising External Routes to Neighbors

Scenario Figure 2- 14	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted)

	● On Router B, configure redistribution of static routes.
B	B# configure terminal B(config)# router rip B(config-router)# redistribute static
Verification	On Router A, check the routing table and verify that the entry 172.10.10.0/24 is loaded.
	A# show ip route rip R 172.10.10.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1

3.4.9 Setting Route Filtering Rules

Configuration Effect

- Routes that do not meet filtering criteria cannot be loaded to the routing table, or advertised to neighbors. In this way, users within the network can be prevented from accessing specified destination networks.

Notes

- The RIP basic functions must be configured.
- In regard to the filtering rules of sent routes, you must configure route redistribution first, and then filter the redistributed routes.

Configuration Steps

Filtering the Received RIP Routing Information

- This function must be configured if it is required to filter received routing information.
- To refuse receiving some specified routes, you can configure the route distribution control list to process all the received route update packets. If no interface is specified, route update packets received on all interfaces will be processed.
- Unless otherwise required, this configuration should be performed on a router that requires route filtering.

Filtering the Sent RIP Routing Information

- This function must be configured if it is required to filter the redistributed routing information that is sent.
- If this command does not contain any optional parameter, route update advertisement control takes effect on all interfaces. If the command contains the interface parameter, route update advertisement control takes effect only on the specified interface. If the command contains other routing process parameters, route update advertisement control takes effect only on the specified routing process.
- Unless otherwise required, this configuration should be performed on a router that requires route filtering.

Verification

- Run the **show ip route rip** command to verify that the routes that have been filtered out are not loaded to the routing table.

Related Commands

Filtering the Received RIP Routing Information

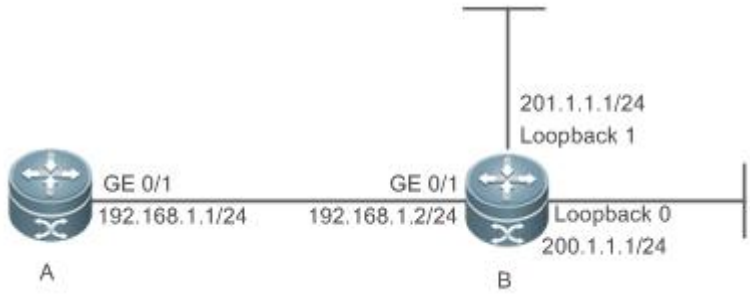
Command Syntax	**distribute-list** { [*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] } **in** [*interface-type interface-number*]
Parameter Description	*access-list-number* | *name*: Specifies the access list. Only routes permitted by the access list can be received. **prefix** *prefix-list-name*: Uses the prefix list to filter routes. **gateway** *prefix-list-name*: Uses the prefix list to filter the route sources. *interface-type interface-number*: Indicates that the distribution list is applied to the specified interface.
Command Mode	Routing process configuration mode
Configuration Usage	N/A

Filtering the Sent RIP Routing Information

Command Syntax	**distribute-list** { [*access-list-number* | *name*] | **prefix** *prefix-list-name* } **out** [*interface* | [**connected** | **ospf** *process-id* |**rip** | **static**]]
Parameter Description	*access-list-number* | *name*: Specifies the access list. Only routes permitted by the access list can be sent. **prefix** *prefix-list-name*: Uses the prefix list to filter routes. *Interface*: Applies route update advertisement control only on the specified interface. **connected**: Applies route update advertisement control only on direct routes introduced through redistribution. **ospf** *process-id*: Applies route update advertisement control only on the routes introduced from OSPF. *process-id* specifies an OSPF process. **rip**: Applies route update advertisement control only on RIP routes. **static**: Applies route update advertisement control only on static routes introduced through redistribution.
Command Mode	Routing process configuration mode
Configuration Usage	N/A

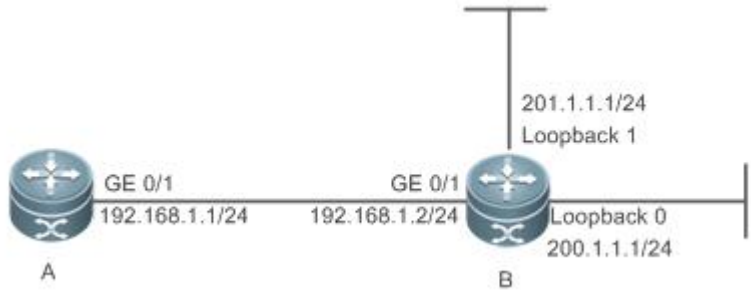
Configuration Example

Filtering the Received RIP Routing Information

Scenario Figure 2- 3- 2	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Enable the RIP routing process to control routes received over the GigabitEthernet 0/1 port and receive only the route 200.1.1.0.

A	A# configure terminal A(config)# router rip A(config-router)# distribute-list 10 in GigabitEthernet 0/1 A(config-router)# no auto-summary A(config)# access-list 10 permit 200.1.1.0 0.0.0.255
Verification	On Router A, check the routing table and verify that only the entry 200.1.1.0/24 exists.
A	A# show ip route rip R 200.1.1.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1

Filtering the Sent RIP Routing Information

Scenario Figure 2- 3- 3	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Enable the RIP routing process to advertise only the route 200.1.1.0/24.
B	B# configure terminal B(config)# router rip B(config-router)# redistribute connected B(config-router)# distribute-list 10 out B(config-router)# version 2 B(config)# access-list 10 permit 200.1.1.0 0.0.0.255
Verification	Check the routing table on Router A, and verify that route in the 200.1.1.0 network segment exists.
A	A# show ip route rip R 200.1.1.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1

Common Errors

- Filtering fails because the filtering rules of the access list are not properly configured.

3.4.10 Modifying Route Selection Parameters

Configuration Effect

- Change the RIP routes to enable the traffic pass through specified nodes or avoid passing through specified nodes.
- Change the sequence that a router selects various types of routes so as to change the priorities of RIP routes.

Notes

- The RIP basic functions must be configured.

Configuration Steps

Modifying the Administrative Distance of a RIP Route

- Optional.
- This configuration is mandatory if you wish to change the priorities of RIP routes on a router that runs multiple unicast routing protocols.

Increasing the Metric of a Received or Sent RIP Route

- Optional.
- Unless otherwise required, this configuration should be performed on a router where the metrics of routes need to be adjusted.

Configuring the Default Metric of an External Route Redistributed to RIP

- Optional.
- Unless otherwise required, this configuration must be performed on an ASBR to which external routes are introduced.

Verification

Run the **show ip rip** command to display the administrative distance currently configured. Run the **show ip rip data** command to display the metrics of redistributed routes to verify that the configuration takes effect.

Related Commands

Modifying the Administrative Distance of a RIP Route

Command Syntax	**distance** *distance* [*ip-address wildcard*]
Parameter Description	*distance*: Sets the administrative distance of a RIP route. The value is an integer ranging from 1 to 255. *ip-address*: Indicates the prefix of the source IP address of the route. *wildcard*: Defines the IP address comparison bit. **0** indicates accurate matching, and **1** indicates that no comparison is performed.
Command Mode	Routing process configuration mode
Configuration Usage	Run this command to configure the administrative distance of a RIP route.

Increasing the Metric of a Received or Sent RIP Route

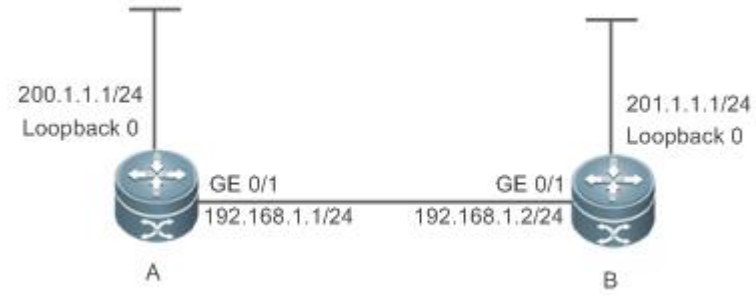
Command Syntax	**offset-list** { *access-list-number* | *name* } { **in** | **out** } *offset* [*interface-type interface-number*]
Parameter Description	*access-list-number* | *name*: Specifies the access list. **In**: Uses the ACL to modify the metric of a received route. **out**: Uses the ACL to modify the metric of a sent route. *offset*: Indicates the offset of the modified metric. The value ranges from 0 to 16. *interface-type*: Uses the ACL on the specified interface. *interface-number*: Specifies the interface number.
Command Mode	Routing process configuration mode
Configuration Usage	Run this command to increase the metric of a received or sent RIP route. If the interface is specified, the configuration takes effect only on the specified interface; otherwise, the configuration takes effect globally.

Configuring the Default Metric of an External Route Redistributed to RIP

Command Syntax	**default-metric** *metric-value*
Parameter Description	*metric-value:* Indicates the default metric. The valid value ranges from 1 to 16. If the value is equal to or greater than 16, the FSOS determines that this route is unreachable.
Command Mode	Routing process configuration mode
Configuration Usage	This command must be used together with the routing protocol configuration command **redistribute**.

Configuration Example

Increasing the Metric of a Received or Sent RIP Route

Scenario Figure 2- 3- 4	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Increase by 7 the metric of each RIP route in the range specified by ACL 7. ● Increase by 7 the metric of each learned RIP route in the range specified by ACL 8.

A	A# configure terminal A(config)# access-list 7 permit host 200.1.1.0 A(config)# access-list 8 permit host 201.1.1.0 A(config)# router rip A(config-router)# offset-list 7 out 7 A(config-router)# offset-list 8 in 7
Verification	Check the routing table on Router A and Router B to verify that the metrics of RIP routes are 8.
A	A# show ip route rip R 201.1.1.0/24 [120/8] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1
B	B# show ip route rip R 200.1.1.0/24 [120/8] via 192.168.1.1, 00:06:11, GigabitEthernet 0/1

3.4.11 Modifying Timers

Configuration Effect

- Change the duration of RIP timers to accelerate or slow down the change of the protocol state or occurrence of an event.

Notes

- The RIP basic functions must be configured.
- Modifying the protocol control parameters may result in protocol running failures. Therefore, you are advised not to modify the timers.

Configuration Steps

Modifying the Update Timer, Invalid Timer, and Flush Timer

This configuration must be performed if you need to adjust the RIP timers.

By adjusting the timers, you can reduce the convergence time and fault rectification time of the routing protocol. For routers connected to the same network, values of the three RIP timers must be the same. Generally, you are advised not to modify the RIP timers unless otherwise required.

Setting timers to small values on a low-speed link brings risks because a lot of Update packets consume the bandwidth. You can set timers to small values generally on the Ethernet or a 2 Mbps (or above) link to reduce the convergence time of network routes.

Unless otherwise required, this configuration should be performed on a router where RIP timers need to be modified.

Setting the Sending Delay Between RIP Route Update Packets

This configuration must be performed if you need to adjust the sending delay between RIP Update packets.

Run the **output-delay** command to increase the sending delay between packets on a high-speed device so that a low-speed device can receive and process all Update packets.

Unless otherwise required, this configuration should be performed on a router where the sending delay needs to be adjusted.

Verification

Run the **show ip rip** command to display the current settings of RIP timers.

Related Commands

Modifying the Update Timer, Invalid Timer, and Flush Timer

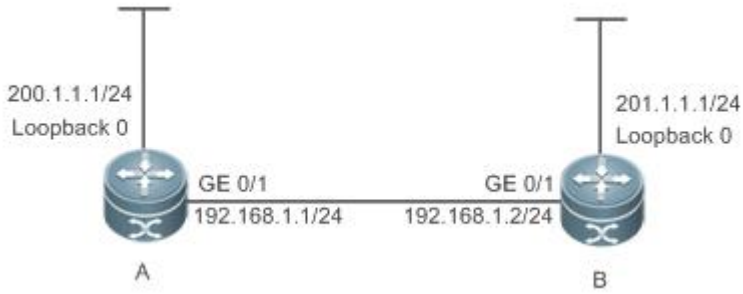
Command Syntax	**timers basic** *update invalid flush*
Parameter Description	*update*: Indicates the route update time in second. It defines the interval at which the device sends the route update packet. Each time an Update packet is received, the invalid timer and flush timer are reset. By default, a routing update packet is sent every 30s. *invalid*: Indicates the route invalid time in second, counted from the last time when a valid update packet is received. It defines the time after which the route in the routing list becomes invalid because the route is not updated. The duration of the invalid timer must be at least three times the duration of the update timer. If no Update packet is received before the invalid timer expires, the corresponding route enters the invalid state. If the Update packet is received before the invalid timer expires, the timer is reset. The default duration of the invalid timer is 180s. *flush*: Indicates the route flushing time in second, counted from the time when the RIP route enters the invalid state. When the flush timer expires, the route in the invalid state will be deleted from the routing table. The default duration of the flush timer is 120s.
Command Mode	Routing process configuration mode
Configuration Usage	By default, the update timer is 30s, the invalid timer is 180s, and the flush timer is 120s.

Setting the Sending Delay Between RIP Route Update Packets

Command Syntax	**output-delay** *delay*
Parameter Description	*delay:* Sets the sending delay between packets in ms. The value ranges from 8 to 50.
Command Mode	Interface configuration mode
Configuration Usage	Normally, a RIP route update packet is 512 bytes long and can contain 25 routes. If the number of routes to be updated exceeds 25, more than one update packet will be sent as fast as possible. When a high-speed device sends a lot of update packets to a low-speed device, the low-speed device may not be able to process all update packets in time, causing a loss of routing information. In this case, you need to run the **output-delay** command to increase the sending delay between packets on a high-speed device so that a low-speed device can receive and process all update packets.

Configuration Example

Setting the Sending Delay Between RIP Route Update Packets

Scenario Figure 2- 18	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Configure the sending delay of update packets on Router A.
A	A# configure terminal A(config)# router rip A(config-router)# output-delay 30
Verification	Capture packets on Router A and compare the sending time of update packets before and after the configuration, and verify that a delay of 30 ms is introduced.

Common Errors

For routers connected to the same network, values of the three RIP timers are not the same.

3.4.12 Enabling GR

Configuration Effect

- When a distributed route switches services from the active board to the standby board, traffic forwarding continues and is not interrupted.
- When the RIP process is being restarted, traffic forwarding continues and is not interrupted.

Notes

- The RIP basic functions must be configured.
- The GR period is at least twice the RIP route update period.
- During the RIP GR process, ensure that the network environment is stable.

Configuration Steps

Configuring the GR Restarter Capability

This configuration must be performed if RIP needs to be gracefully restarted to ensure data forwarding during hot standby switchover.

The GR function is configured based on the RIP process. You can configure different parameters for different RIP processes based on the actual conditions.

The GR period is the maximum time from restart of the RIP process to completion of GR. During this period, the forwarding table before the restart is retained, and the RIP route is restored so as to restore the RIP state before the restart. After the restart period expires, RIP exits from the GR state and performs common RIP operations.

Unless otherwise required, this configuration should be performed on every router that needs to be gracefully restarted.

Verification

- Run the **show ip rip** command to display the GR state and configured time.
- Trigger a hot standby switchover, and verify that data forwarding is not interrupted.

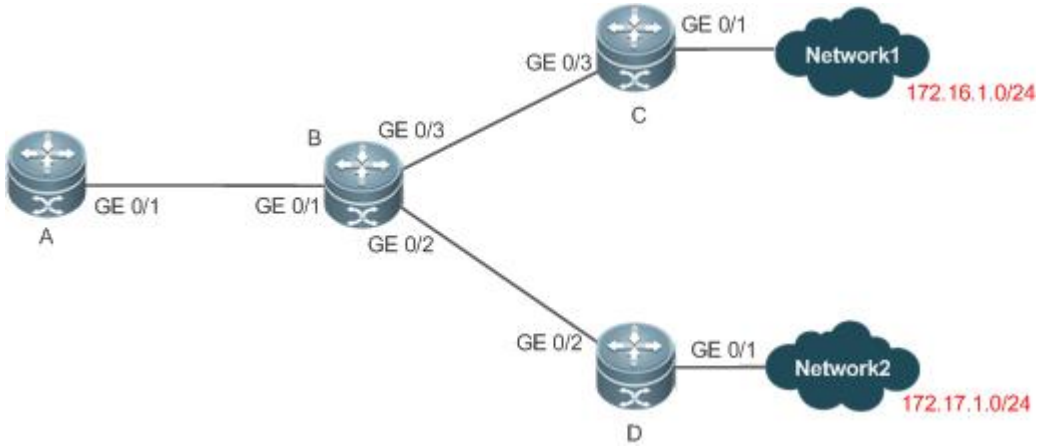
Related Commands

Configuring the GR Restarter Capability

Command Syntax	**graceful-restart** [**grace-period** *grace-period*]
Parameter Description	**graceful-restart**: Enables the GR function. **grace-period**: Explicitly configures the grace period. *grace-period*: Indicates the GR period. The value ranges from 1s to 1800s. The default value is twice the update time or 60s, whichever is the smaller.
Command Mode	Routing process configuration mode
Configuration Usage	This command allows you to explicitly modify the GR period. Note that GR must be completed after the update timer of the RIP route expires and before the invalid timer of the RIP route expires. An inappropriate GR period cannot ensure uninterrupted data forwarding during the GR process. A typical case is as follows: If the GR period is longer than the duration of the invalid timer, GR is not completed when the invalid timer expires. The route is not re-advertised to the neighbor, and forwarding of the route of the neighbor stops after the invalid timer expires, causing interruption of data forwarding on the network. Unless otherwise required, you are advised not to adjust the GR period. If it is necessary to adjust the GR period, ensure that the GR period is longer than the duration of the update timer but shorter than the duration of the invalid timer based on the configuration of the **timers basic** command.

Configuration Example

Configuring the GR Restarter Capability

Scenario Figure 2- 19	 **Remarks**: The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 B: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 GE 0/3 192.168.3.1 C: GE 0/1 192.168.4.2 GE 0/3 192.168.3.2 D: GE 0/1 192.168.5.2 GE 0/2 192.168.2.2
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● On Router B, enable the GR function.
	B# configure terminal B(config)# router rip B(config-router)# graceful-restart grace-period 90
Verification	● Trigger a hot standby switchover on Router B, and verify that the routing tables of destination Network 1 and Network 2 remain unchanged on Router A during the switchover. ● Trigger a hot standby switchover on Router B, ping destination Network 1 from Router A, and verify that traffic forwarding is not interrupted during the switchover.

3.5 Monitoring

Displaying

Description	Command
Displays the basic information about a RIP process.	**show ip rip**
Displays the RIP routing table.	**show ip rip database** [*network-number network-mask*] [**count**]
Displays information about external routes redistributed by RIP.	**show ip rip external** [**connected** | **ospf** *process-id* | **static**]
Displays the RIP interface information.	**show ip rip interface** [*interface-type interface-number*]
Displays the RIP neighbor information.	**show ip rip peer** [*ip-address*]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs events that occur when the RIP process is running.	**debug ip rip event**
Debugs interaction with the NSM process.	**debug ip rip nsm**
Debugs the sent and received packets.	**debug ip rip packet** [**interface** *interface-type interface-number* | **recv** | **send**]
Debugs the RIP GR process.	**debug ip rip restart**
Debugs the route changes of the RIP process.	**debug ip rip route**

4 Configuring RIPng

4.1 Overview

RIP next generation (RIPng) is a unicast routing protocol that applies to IPv6 networks. RIPng-enabled routers exchange routing information to obtain routes to remote networks.

As an Interior Gateway Protocol (IGP), RIPng can run only within the autonomous system (AS) and is applicable to small-sized networks with routes no more than 16 hops.

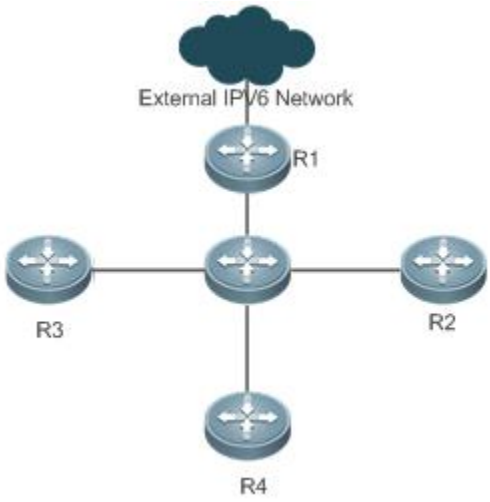
Protocols and Standards

- RFC2080: Defines the RIPng.

4.2 Application

RIPng is generally used on some small-sized networks, such as office networks of small companies.

As shown in the following figure, the company builds an IPv6 network, on which all routers support IPv6. The network is small in size, but the workload is still heavy if the network is maintained manually. In this case, RIPng can be configured to adapt to topological changes of the small-sized network, which reduces the workload.



4.3 Features

Basic Concepts

IGP and EGP

IGP runs within an AS. For example, RIPng is a type of IGP.

Exterior Gateway Protocol (EGP) runs between ASs. For example, BGP is a type of EGP.

Feature

Feature	Description
RIPng and RIP	RIPng is an extension of RIPv2 on the basis of IPv6. Both are similar in functions and configurations.
Exchanging Routing Information	By exchanging routing information, RIPng-enabled devices can automatically obtain routes to a remote network and update routes in real time.

Routing Algorithm	RIPng is a protocol based on the distance-vector algorithm. It uses the vector addition method to compute the routing information.
Avoiding Route Loops	RIPng uses functions, such as split horizon and poison reverse, to avoid route loops.

4.3.1 RIPng and RIP

RIP applies to IPv4 networks. Two RIP versions are available, including RIPv1 and RIPv2.
RIPng is an extension of RIPv2 on the basis of IPv6. Both are similar in functions and configurations.

Working Principle

RIPv2

RIPv2 packets are multicast. The multicast address is 224.0.0.9, and the UDP port ID is 520. RIPv2 can identify the subnet mask.

RIPng

RIPng packets are multicast. The multicast address is FF02::9, the source address is FE80::/10, and the UDP port ID is 521. RIPng can identify the subnet mask.

This chapter describes functions and configurations of RIPng. For details about RIPv2, see "Configuring RIP".

Related Configuration

Enabling the RIPng Process

By default, the RIPng process is disabled.
Run the **ipv6 router rip** command to enable the RIPng process.
You must enable the RIPng process on a device; otherwise, all functions related to RIPng cannot take effect.

Running RIPng on an Interface

By default, RIPng does not run on an interface.
Run the **ipv6 rip enable** command to run RIPng on an interface.
After RIPng runs on an interface, RIPng packets can be exchanged on the interface and RIPng can learn routes to the network segments directly connected to the device.

Prohibiting an Interface from Sending or Receiving Packets

By default, a RIPng-enabled interface is allowed to send and receive RIPng packets.
Run the **passive-interface** command to prohibit an interface from sending RIPng packets.

4.3.2 Exchanging Routing Information

Compared with static routing, the dynamic routing protocol has a significant advantage, that is, by exchanging routing information, devices can automatically obtain routes to a remote network and update the routes in real time.

Working Principle

Initialization

After RIPng is enabled on a router, the router sends a request packet to its neighbor router, requesting for all routing information, that is, the routing table. After receiving the request message, the neighbor router returns a response packet containing the local routing

table. After receiving the response packet, the router updates the local routing table, and sends an update packet to the neighbor router, informing the neighbor router of the route update information. After receiving the update packet, the neighbor router updates the local routing table, and sends the update packet to other adjacent routers. After a series of updates, all routers can obtain and retain the latest routing information.

Periodical Update

By default, periodical update is enabled for RIPng. Adjacent routers exchange complete routing information with each other every 30s (update timer), that is, the entire routing table is sent to neighbor routers.

For every non-local route, if the route is not updated within 180s (invalid timer), the metric of the route is changed to 16 (unreachable). If the route is still not updated in the next 120s (flush timer), the route is deleted from the routing table.

Default Route

In the routing table, a route to the destination network ::/0 is called default route.
The default route can be learned from a neighbor router, or sent to a neighbor router.

Route Redistribution

For RIPng, other types of routes (such as direct routes, static routes, and routes of other routing protocols) are called external routes. External routes (excluding the default route) can be redistributed to RIPng and advertised to neighbors.

Route Filtering

Filtering conditions can be configured to limit the routing information exchanged between adjacent routers. Only the routing information that meets filtering conditions can be sent or received.

Related Configuration

RIPng Timers

By default, the update timer is 30s, the invalid timer is 180s, and the flush timer is 120s.
Run the **timers basic** command to modify durations of RIPng timers.
Increasing the duration of the flush timer can reduce the route flapping. Decreasing the duration of the flush timer helps accelerate route convergence.
The durations of RIPng timers must be consistent on adjacent routers. Unless otherwise required, you are advised not to modify the RIPng timers.

Default Route

Run the **ipv6 rip default-information** command to advertise the default route to neighbors on an interface.

Route Redistribution

Run the **redistribute** command to redistribute external routes (excluding the default route) to RIPng and advertise them to neighbors.

Route Filtering

Run the **distribute-list out** command to set filtering rules to limit the routing information sent by the device.
Run the **distribute-list in** command to set filtering rules to limit the routing information received by the device.

4.3.3 Routing Algorithm

RIPng is a protocol based on the distance-vector algorithm. It uses the vector addition method to compute the routing information.

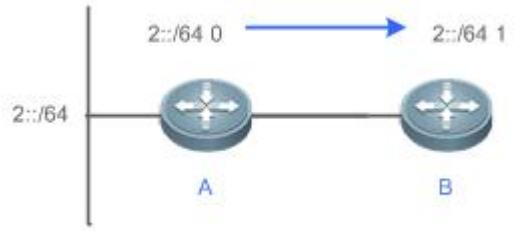
Working Principle

Distance-Vector Algorithm

RIPng is a protocol based on the distance-vector algorithm. The distance-vector algorithm treats a route as a vector that consists of the destination network and distance (metric). The router obtains a route from its neighbor and adds the distance vector from itself to the neighbor to the route to form its own route.

RIPng uses the hop count to evaluate the distance (metric) to the destination network. By default, the hop count from a router to its directly connected network is 0, the hop count from a router to a network that can be reached through a router is 1, and so on. That is, the metric is equal to the number of routers from the local network to the destination network. To restrict the convergence time, RIPng stipulates that the metric must be an integer between 0 and 15. If the metric is equal to or greater than 16, the destination network or host is unreachable. For this reason, RIPng cannot be applied to a large-scale network.

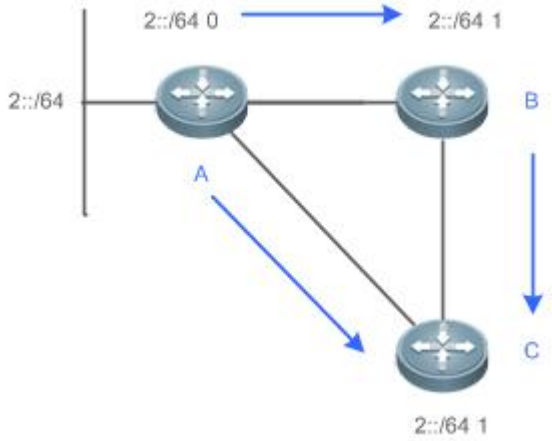
As shown in the following figure, Router A is connected to the network 2::/64. Router B obtains the route (2::/64, 0) from Router A and adds the metric 1 to the route to obtain its own route (2::/64, 1), and the next hop points to Router A.



Selecting the Optimum Route

RIPng selects an optimum route based on the following principle: If multiple routes to the same destination network is available, a router preferentially selects the route with the smallest metric.

As shown in the following figure, Router A is connected to the network 2::/64. Router C obtains the route (2::/64, 0) from Router A and the route (2::/64, 1) from Router B. Router C will select the route that is obtained from Router A and add metric 1 to this route to form its own route (2::/64, 1), and the next hop points to Router A.



When routes coming from different sources exist on a router, the route with the smaller distance is preferentially selected.

Route Source	Default Distance
Directly-connected network	0
Static route	1
OSPF route	110
IS-IS route	115
RIPng route	120
Unreachable route	255

Related Configuration

Modifying the Distance

By default, the distance of a RIPng route is 120.

Run the **distance** command to modify the distance of a RIPng route.

Modifying the Metric

For a RIPng route that is proactively discovered by a device, the default metric is equal to the number of hops from the local network to the destination network. The metric offset of the interface is 1.

For a RIPng router that is manually configured (default route or redistributed route), the default metric is 1.

Run the **ipv6 rip metric-offset** command to modify the metric offset of the interface.

Run the **default-metric** command to modify the default metric of an external route (redistributed route).

Run the **redistribute** command to modify the metric of an external route (redistributed route) when advertising this route.

Run the **ipv6 rip default-information** command to modify the metric of a default route when advertising the default route.

4.3.4 Avoiding Route Loops

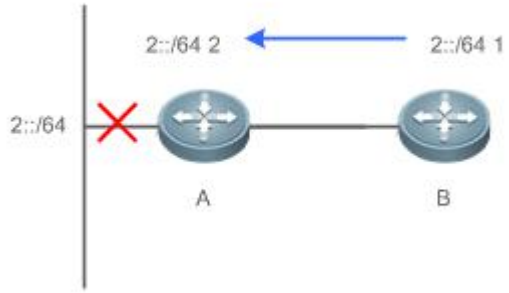
RIPng uses functions, such as split horizon and poison reverse, to avoid route loops.

Working Principle

Route Loop

A RIPng route loop occurs due to inherent defects of the distance-vector algorithm.

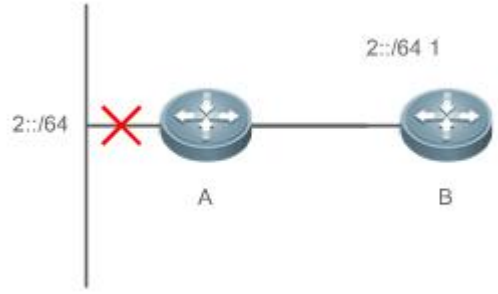
As shown in the following figure, Router A is connected to the network 2::/64, and sends an update packet every 30s. Router B receives the route to 2::/64 from Router A every 30s. If Router A is disconnected from 2::/64, the route to 2::/64 will be deleted from the routing table on Router A. Next time, the update packet sent by Router A no longer contains this route. As Router B does not receive an update packet related to 2::/64, Router B determines that the route to 2::/64 is valid within 180s and uses the update packet to send this route to Router A. As the route to 2::/64 does not exist on Router A, the route learned from Router B is added to the routing table. Router B determines that data can reach 2::/64 through Router A, and Router A determines that data can reach 2::/64 through Router B. In this way, a route loop is formed.



Split Horizon

Split horizon can prevent route loops. After split horizon is enabled, a route received on this interface will not be sent out from this interface.

As shown in the following figure, after split horizon is enabled on Router B, Router B will not send the route to 2::/64 back to Router A. Router B will learn 180s later that 2::/64 is not reachable.

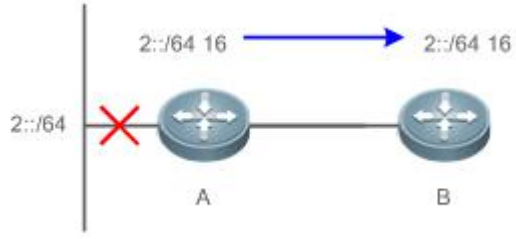


Poison Reverse

Poison reverse can also prevent route loops. Compared with slit horizon, poison reverse is more reliable, but brings more protocol packets, which makes network congestion more severe.

After poison reverse is enabled on an interface, a route received from this interface will be sent out from this interface again, but the metric of this router will be changed to 16 (unreachable).

As shown in the following figure, after poison reverse is enabled on Router A, if Route A detects a disconnection from 2::/64, Router A will not delete the route to 2::/64. Instead, Router A changes the number of hops to 16, and advertises the route through the update packet. On receiving the update packet, Router B learns that 2::/64 is not reachable.



Related Configuration

Split Horizon

By default, split horizon is enabled.

Run the **no split-horizon** command to disable split horizon.

Poison Reverse

By default, poison reverse is disabled.

Run the **split-horizon poisoned-reverse** command to enable poison reverse. (After poison reverse is enabled, split horizon is automatically disabled.)

4.4 Configuration

Configuration	Related Commands	
Configuring RIPng Basic Functions	(Mandatory) It is used to build a RIPng routing domain.	
	ipv6 router rip	Enables a RIPng routing process and enters routing process configuration mode.
	ipv6 rip enable	Runs RIPng on an interface.
	split-horizon	Enables split horizon or poison reverse.
	passive-interface	Configures a passive interface.
Advertising the Default Route or External Routes	Optional.	
	ipv6 rip default-information	Advertise the default route to neighbors on an interface.
	redistribute	Redistributes routes and advertising external routes to neighbors.
Setting Route Filtering Rules	Optional.	
	distribute-list in	Filters the received RIPng routing information.
	distribute-list out	Filters the sent RIPng routing information.
Modifying Route Selection Parameters	Optional.	
	distance	Modifies the administrative distance of a RIPng route.
	ipv6 rip metric-offset	Modifies the metric offset on an interface.
	default-metric	Configure the default metric for route redistribution.
Modifying Timers	Optional.	
	timers	Modifies the update timer, invalid timer, and flush timer of RIPng.

4.4.1 Configuring RIPng Basic Functions

Configuration Effect

- Build a RIPng routing domain on the network.
- Routers in the domain obtain routes to a remote network through RIPng.

Notes

- IPv6 addresses must be configured.
- IPv6 unicast routes must be enabled.

Configuration Steps

Enabling a RIPng Routing Process

- Mandatory.
- Unless otherwise required, perform this configuration on every router in the RIPng routing domain.

Running RIPng on an Interface

- Mandatory.
- Unless otherwise required, perform this configuration on every interconnected interface of routers in the RIPng routing domain.

Enabling Split Horizon or Poison Reverse

- By default, split horizon is enabled and poison reverse is disabled.
- Unless otherwise required, enable split horizon on every interface connected to the broadcast network, such as the Ethernet. (Retain the default setting.)
- Unless otherwise required, enable split horizon on every interface connected to the point-to-point (P2P) network, such as the PPP and HDLC. (Retain the default setting.)
- It is recommended that split horizon and poison reverse be disabled on an interface connected to a non-broadcast multi-access network, such as FR and X.25; otherwise, some devices cannot learn the complete routing information.
- If the secondary IP address is configured for an interface connected to a non-broadcast, it is recommended that split horizon and poison reverse be disabled.

Configuring a Passive Interface

- This configuration is recommended.
- Use the passive interface to set the boundary of the RIPng routing domain. The network segment of the passive interface belongs to the RIPng routing domain, but RIPng packets cannot be sent over the passive interface.
- If RIPng routes need to be exchanged on an interface (such as the router interconnect interface) in the RIPng routing domain, this interface cannot be configured as a passive interface.

Verification

- Check the routing table on a router to verify that the route to a remote network can be obtained through RIPng.

Related Commands

Enabling a RIPng Routing Process

Command	ipv6 router rip
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This command is used to create a RIPng routing process and enter routing process configuration mode.

Running RIPng on an Interface

Command	ipv6 rip enable
Parameter	N/A

Description	
Command Mode	Interface configuration mode
Usage Guide	The configuration for running the RIPng on an interface is different from that of RIPv2. In RIPv2, the **network** command is configured in routing process configuration mode to define an IP address range. If the IP address of an interface belongs to this IP address range, RIP automatically runs on this interface.

Enabling Split Horizon

Command	**split-horizon** [**poisoned-reverse**]
Parameter Description	**poisoned-reverse**: Indicates that the split horizon function contains the poison reverse function.
Command Mode	Routing process configuration mode
Usage Guide	Run the **show ipv6 rip** command to check whether split horizon is enabled. The configuration is different from that of RIPv2. In RIPv2, the split horizon function is configured in interface configuration mode.

Configuring a Passive Interface

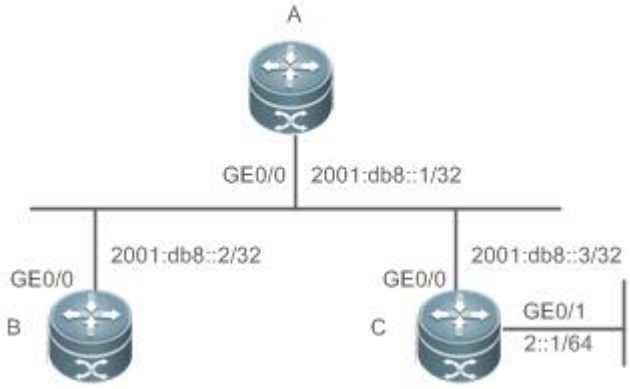
Command	**passive-interface** { **default** | *interface-type interface-num* }
Parameter Description	**default:** Indicates all interfaces. ***interface-type interface-num***: Specifies an interface.
Command Mode	Routing process configuration mode
Usage Guide	First, run the **passive-interface default** command to configure all interfaces as passive interfaces. Then, run the **no passive-interface** *interface-type interface-num* command so that the interfaces used for interconnection between routers in the domain are not passive interface.

Displaying the IP Routing Table

Command	**show ipv6 route**
Parameter Description	N/A
Command Mode	Privileged EXEC mode or global configuration mode
Usage Guide	Check whether the routing table contains any route to a remote network that is learned through RIPng.

Configuration Example

Building a RIPng Routing Domain

Scenario **Figure 4- 1**	
Configuration Steps	● Configure IPv6 addresses on all routers. ● Enable RIPng on all routers.
A	A# configure terminal Enter configuration commands, one per line. End with CNTL/Z. A(config)# ipv6 router rip A(config-router)# exit A(config)# interface GigabitEthernet 0/0 A(config-if-GigabitEthernet 0/0)# ipv6 address 2001:db8::1/32 A(config-if-GigabitEthernet 0/0)# ipv6 rip enable
B	B# configure terminal Enter configuration commands, one per line. End with CNTL/Z. B(config)# ipv6 router rip B(config-router)# exit B(config)# interface GigabitEthernet 0/0 B(config-if-GigabitEthernet 0/0)# ipv6 address 2001:db8::2/32 B(config-if-GigabitEthernet 0/0)# ipv6 rip enable
C	C# configure terminal Enter configuration commands, one per line. End with CNTL/Z. C(config)# ipv6 router rip C(config-router)# exit C(config)# interface GigabitEthernet 0/0 C(config-if-GigabitEthernet 0/0)# C(config-if-GigabitEthernet 0/0)# ipv6 address 2001:db8::3/32 C(config-if-GigabitEthernet 0/0)# ipv6 rip enable

	C(config)# interface GigabitEthernet 0/1 C(config-if-GigabitEthernet 0/1)# ipv6 address 2::1/64 C(config-if-GigabitEthernet 0/1)# ipv6 rip enable
Verification	Check the routing tables on Router A, Router B, and Router C. The routing tables should contain routes to a remote network that are learned through RIPng.
A	A# show ipv6 route IPv6 routing table name - Default - 6 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area R 2::/64 [120/2] via FE80::2D0:F8FF:FEFB:D521, GigabitEthernet 0/0 C 2001:DB8::/32 via GigabitEthernet 0/0, directly connected L 2001:DB8::1/128 via GigabitEthernet 0/0, local host C FE80::/10 via ::1, Null0 C FE80::/64 via GigabitEthernet 0/0, directly connected L FE80::2D0:F8FF:FEFB:E7CE/128 via GigabitEthernet 0/0, local host
B	B# show ipv6 route IPv6 routing table name - Default - 6 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area R 2::/64 [120/2] via FE80::2D0:F8FF:FEFB:D521, GigabitEthernet 0/0 C 2001:DB8::/32 via GigabitEthernet 0/0, directly connected

	L 2001:DB8::2/128 via GigabitEthernet 0/0, local host C FE80::/64 via GigabitEthernet 0/0, directly connected L FE80::2D0:F8FF:FEFB:C9BA/128 via GigabitEthernet 0/0, local host
C	FS# show ipv6 route IPv6 routing table name - Default - 9 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area C 2::/64 via GigabitEthernet 0/1, directly connected L 2::2/128 via GigabitEthernet 0/1, local host C 2001:DB8::/32 via GigabitEthernet 0/0, directly connected L 2001:DB8::3/128 via GigabitEthernet 0/0, local host C FE80::/10 via ::1, Null0 C FE80::/64 via GigabitEthernet 0/0, directly connected L FE80::2D0:F8FF:FEFB:D521/128 via GigabitEthernet 0/0, local host C FE80::/64 via GigabitEthernet 0/1, directly connected L FE80::2D0:F8FF:FEFB:D521/128 via GigabitEthernet 0/1, local host

Common Errors

- The IPv6 address is not configured on an interface.
- The interface used for interconnection between devices is configured as a passive interface.

4.4.2 Advertising the Default Route or External Routes

Configuration Effect

- In the RIPng domain, introduce a unicast route of another AS so that the unicast routing service to this AS can be provided for users in the RIPng domain.
- In the RIPng domain, inject a default route to another AS so that the unicast routing service to this AS can be provided for users in the RIPng domain.

Notes

- The RIPng basic functions must be configured.

Configuration Steps

Configuring External Route Redistribution

- Optional.
- Perform this configuration if external routes of the RIPng domain should be introduced to the AS border router (ASBR).

Generating a Default Route

- Optional.
- Perform this configuration if the default route should be introduced to an ASBR so that other routers in the RIPng domain access other AS domains through this ASBR by default.

Verification

- Run the **show ipv6 route rip** command on a non-ASBR to check whether the external routes of the domain and default route have been loaded.

Related Commands

Advertising the Default Route to Neighbors on an Interface

Command	**ipv6 rip default-information** { **only**|**originate** } [**metric** *metric-value*]
Parameter Description	**only**: Advertises only IPv6 default route. **originate**: Advertises the IPv6 default route and other routes. **metric** *metric-value*: Indicates the metric of the default route. The value ranges from 1 to 15. The default value is 1.
Command Mode	Interface configuration mode
Usage Guide	After this command is configured on the interface, an IPv6 default route is advertised to the external devices through this interface, but the route itself is not added to the route forwarding table or the device and the RIPng route database. To prevent occurrence of a route loop, once this command is configured on an interface, RIPng refuses to receive the default route updates advertised by neighbors.

Redistributing Routes and Advertising External Routes to Neighbors

Command	**redistribute** { **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **static** } [**metric** *metric-value* | **route-map** *route-map-name*]
Parameter Description	**bgp**: Indicates redistribution from BGP. **Connected**: Indicates redistribution from direct routes. **isis** [*area-tag*]: Indicates redistribution from IS-IS. *area-tag* indicates the IS-IS process ID. **ospf** *process-id*: Indicates redistribution from OSPF. *process-id* indicates the OSPF process ID. The value ranges from 1 to 65535. **static**: Indicates redistribution from static routes. **metric** *metric-value*: Sets the metric of the route redistributed to the RIPng domain. **route-map** *route-map-name*: Sets the redistribution filtering rules.
Command Mode	Routing process configuration mode

Usage Guide	During route redistribution, it is not necessary to convert the metric of one routing protocol to the metric of another routing protocol because different routing protocols use completely different metric measurement methods. RIP measures the metric based on the hop count, and OSPF measures the metric based on the bandwidth. Therefore, the computed metrics cannot be compared with each other.

Configuration Example

Scenario	
Configuration Steps	● Configure the interface IPv6 addresses on all routers. (Omitted) ● Configure the RIPng basic functions on all routers. (Omitted) ● On Router B, configure redistribution of static routes. ● On the GE0/1 interface of Router A, configure advertisement of the default route.
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ipv6 rip default-information originate
B	B# configure terminal B(config)# ipv6 router rip B(config-router)# redistribute static
Verification	● Check the routing tables on Router A and Router B, and confirm that Router A can learn the route 3001:10:10::/64, and Router B can learn the default route ::/0.
A	A# show ipv6 route rip IPv6 routing table name - Default - 17 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area R 3001:10:10::/64 [120/2] via FE80::2D0:F8FF:FE22:334A, GigabitEthernet 0/1

B	B# show ipv6 route rip IPv6 routing table name - Default - 17 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area R ::/0 [120/2] via FE80::21A:A9FF:FE41:5B06, GigabitEthernet 0/1

4.4.3 Setting Route Filtering Rules

Configuration Effect

- Routes that do not meet filtering criteria cannot be loaded to the routing table, or advertised to neighbors. In this way, users within the network can be prevented from accessing specified destination networks.

Notes

- The RIPng basic functions must be configured.

Configuration Steps

Filtering the Received RIP Routing Information

- To refuse receiving some specified routes, you can configure the route distribution control list to process all the received route update packets. If no interface is specified, route update packets received on all interfaces will be processed.

Filtering the Sent RIP Routing Information

- If this command does not contain any optional parameter, route update advertisement control takes effect on all interfaces. If the command contains the interface parameter, route update advertisement control takes effect only on the specified interface. If the command contains other routing process parameters, route update advertisement control takes effect only on the specified routing process.

Verification

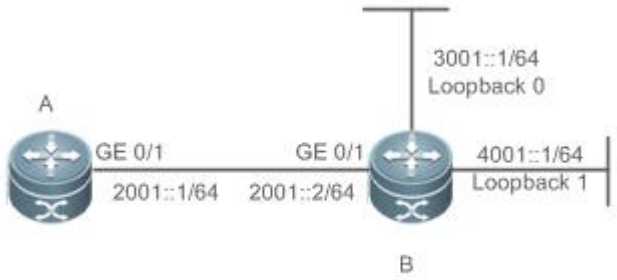
- Run the **show ipv6 route rip** command to check that the routes that have been filtered out are not loaded to the routing table.

Related Commands

Command	**distribute-list prefix-list** *prefix-list-name* { **in** | **out** } [*interface-type interface-name*]
Parameter Description	**prefix-list** *prefix-list-name:* Indicates the name of the prefix list, which is used to filter routes. **in** | **out:** Specifies update routes (received or sent routes) that are filtered. *interface-type interface-name:* Indicates that the distribution list is applied to the specified interface.
Command	Routing process configuration mode

Mode	
Usage Guide	N/A

Configuration Example

Scenario	
Configuration Steps	● Configure the interface IPv6 addresses on all routers. (Omitted) ● Configure the RIPng basic functions on all routers. (Omitted) ● On router A, configure route filtering.
A	A# configure terminal A(config)# ipv6 prefix-list hello permit 4001::/64 A(config)# ipv6 router rip A(config-router)# distribute-list prefix-list hello in
Verification	● Check that Router A can learn only the route to 4001::/64.
A	A# show ipv6 route rip IPv6 routing table name - Default - 17 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area R 4001::/64 [120/2] via FE80::2D0:F8FF:FE22:334A, GigabitEthernet 0/1

4.4.4 Modifying Route Selection Parameters

Configuration Effect

- Change the RIPng routes to enable the traffic pass through specified nodes or avoid passing through specified nodes.
- Change the sequence that a router selects various types of routes so as to change the priorities of RIPng routes.

Notes

- The RIPng basic functions must be configured.

Configuration Steps

Modifying the Administrative Distance of a RIPng Route

- Optional.
- Perform this configuration if you wish to change the priorities of RIPng routes on a router that runs multiple unicast routing protocols.

Modifying the Metric Offset on an Interface

- Optional.
- Unless otherwise required, perform this configuration on a router where the metrics of routes need to be adjusted.

Configuring the Default Metric of an External Route Redistributed to RIPng

- Optional.
- Unless otherwise required, perform this configuration on an ASBR to which external routes are introduced.

Verification

- Run the **show ipv6 rip** command to display the administrative distance of RIPng routes.
- Run the **show ipv6 rip data** command to display the metrics of external routes redistributed to RIPng.

Related Commands

Modifying the Administrative Distance of a RIPng Route

Command	**distance** *distance*
Parameter Description	*distance*: Sets the administrative distance of a RIPng route. The value is an integer ranging from 1 to 254.
Command Mode	Routing process configuration mode
Usage Guide	Run this command to set the administrative distance of a RIPng route.

Modifying the Metric Offset on an Interface

Command	**ipv6 rip metric-offset** *value*
Parameter Description	*value*: Indicates the interface metric offset. The value ranges from 1 to 16.
Command Mode	Routing process configuration mode
Usage Guide	Before a route is added to the routing table, the metric of the route must be added with the metric offset set on the interface. You can control the use of a route by setting the interface metric offset.

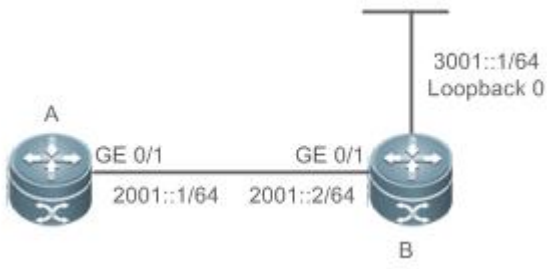
Configuring the Default Metric of an External Route Redistributed to RIPng

Command	**default-metric** *metric*
Parameter Description	*metric*: Indicates the default metric. The valid value ranges from 1 to 16. If the value is equal to or greater than 16, the FSOS determines that this route is unreachable.
Command Mode	Global configuration mode
Usage Guide	If the metric is not specified during redistribution of a routing protocol process, RIPng uses the metric defined by the

	default-metric command. If the metric is specified, the metric defined by the **default-metric** command is overwritten by the specified metric. If this command is not configured, the value of **default-metric** is 1.

Configuration Example

Modifying the Administrative Distance of a RIPng Route

Scenario	
Configuration Steps	● Configure the interface IPv6 addresses on all routers. (Omitted) ● Configure the RIPng basic functions on all routers. (Omitted) ● On Router A, set the administrative distance of a RIPng route to 160.
	A# configure terminal A(config)# ipv6 router rip A(config-router)# distance 160
Verification	● On Router A, check whether the administrative distance of a RIPng route is 160.
	A# show ipv6 route rip | in 3001::/64 R 3001::/64 [160/2] via FE80::2D0:F8FF:FE22:334A, GigabitEthernet 0/1

4.4.5 Modifying Timers

Configuration Effect

- Change the duration of RIPng timers to accelerate or slow down the change of the protocol state or occurrence of an event.

Notes

- The RIPng basic functions must be configured.
- Modifying the protocol control parameters may result in protocol running failures. Therefore, you are advised not to modify the timers.

Configuration Steps

Modifying the Update Timer, Invalid Timer, and Flush Timer

- Mandatory.
- Unless otherwise required, perform this configuration on a router where RIPng timers need to be modified.

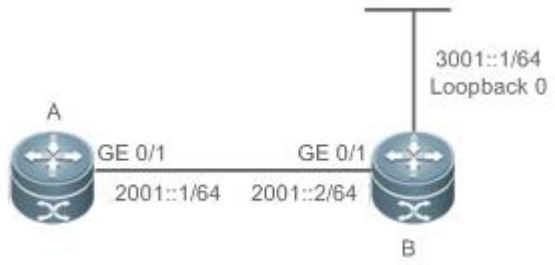
Verification

- Run the **show ipv6 rip** command to display settings of timers.

Related Commands

Command	**timers** *update invalid flush*
Parameter Description	*Update:* Indicates the route update time in second. It defines the interval at which the device sends the route update packet. Each time an update packet is received, the invalid timer and flush timer are reset. By default, a route update packet is sent every 30s. *Invalid:* Indicates the route invalid time in second, counted from the last time when a valid update packet is received. It defines the time after which the route in the routing list becomes invalid because the route is not updated. The duration of the invalid timer must be at least three times the duration of the update timer. If no update packet is received before the invalid timer expires, the corresponding route enters the invalid state. If the update packet is received before the invalid timer expires, the timer is reset. The default duration of the invalid timer is 180s. *Flush:* Indicates the route flushing time in second, counted from the time when the RIPng route enters the invalid state. When the flush timer expires, the route in the invalid state will be deleted from the routing table. The default duration of the flush timer is 120s.
Command Mode	Routing process configuration mode
Usage Guide	By default, the update timer is 30s, the invalid timer is 180s, and the flush timer is 120s.

Configuration Example

Scenario	
Configuration Steps	● Configure the interface IPv6 addresses on all routers. (Omitted) ● Configure the RIPng basic functions on all routers. (Omitted) ● On Router A, configure the update timer, invalid timer, and flush timer.
B	B# configure terminal B(config)# ipv6 router rip B(config-router)# timers 10 30 90
Verification	● On Router B, check the settings of RIPng timers.

B	B# show ipv6 rip Routing Protocol is "RIPng" Sending updates every 10 seconds with +/-50%, next due in 12 seconds Timeout after 30 seconds, garbage collect after 90 seconds Outgoing update filter list for all interface is: not set Incoming update filter list for all interface is: not set Default redistribution metric is 1 Default distance is 120 Redistribution: Redistributing protocol connected Default version control: send version 1, receive version 1 Interface Send Recv GigabitEthernet 0/1 1 1 Routing Information Sources: Gateway: fe80::2d0:f8ff:fe22:334a Distance: 120 Last Update: 00:00:02 Bad Packets: 0 Bad Routes: 0

Common Errors

- Settings of RIPng timers on devices connected to the same network are inconsistent. Consequently, routes cannot be learned properly.

4.5 Monitoring

Displaying

Description	Command
Displays information about the RIPng process.	**show ipv6 rip**
Displays the RIPng routing table.	**show ipv6 rip database**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs RIPng.	**debug ipv6 rip** [interface *interface-type interface-num* | nsm | restart | event [ipsec]]

5 Configuring OSPFv2

5.1 Overview

Open Shortest Path First (OSPF) is an Interior Gateway Protocol (IGP) that is used within the Autonomous System (AS) to allow routers to obtain a route to a remote network.

OSPF Version 2 (OSPFv2) is applicable to IPv4. The protocol running mechanism and most configurations are the same.

OSPF has the following characteristics:

- Wide scope of application: OSPF is applicable to a larger-scale network that supports hundreds of routers.
- Fast convergence: Once the network topology changes, notifications can be quickly sent between routers to update routes.
- No self-loop: Only the link status information is synchronized between routers. Each router computes routes independently, and a self-loop will not occur.
- Area division: A large routing domain is divided into multiple small areas to save system resources and network bandwidth and ensure stability and reliability of routes.
- Route classification: Routes are classified into several types to support flexible control.
- Equivalent routes: OSPF supports equivalent routes.
- Authentication: OSPF supports packet authentication to ensure security of protocol interaction.
- Multicast transmission: Protocol packets are sent using the multicast address to avoid interfering with irrelevant entities and save system resources.

Unless otherwise specified, "OSPF" in the following descriptions refers to OSPFv2.

Protocols and Standards

RFC2328	This memo documents version 2 of the OSPFprotocol. OSPF is a link-state routing protocol.
RFC 2370	This memo defines enhancements to the OSPFprotocol to support a new class of link-stateadvertisements (LSA) called Opaque LSAs.Opaque LSAs provide a generalized mechanismto allow for the future extensibility of OSPF.
RFC3137	This memo describes a backward-compatibletechnique that may be used by OSPF (OpenShortest Path First) implementations to advertiseunavailability to forward transit traffic or to lowerthe preference level for the paths through such arouter.
RFC3623	This memo documents an enhancement to theOSPF routing protocol, whereby an OSPF routercan stay on the forwarding path even as its OSPFsoftware is restarted.
RFC3630	This document describes extensions to the OSPFprotocol version 2 to support intra-area TrafficEngineering (TE), using Opaque Link StateAdvertisements.
RFC3682	The use of a packet's Time to Live (TTL) (IPv4)or Hop Limit (IPv6) to protect a protocol stackfrom CPU-utilization based attacks has beenproposed in many settings.
RFC3906	This document describes how conventional hop-by-hop link-state routing protocols interact withnew Traffic Engineering capabilities to createInterior Gateway Protocol (IGP) shortcuts.
RFC4576	This document specifies the necessary procedure,using one of the options bits in the LSA (Link StateAdvertisements) to indicate that an LSA hasalready been forwarded by a PE and should beignored by any other PEs that see it.

RFC4577	This document extends that specification byallowing the routing protocol on the PE/CEinterface to be the OSPF protocol.
RFC4750	This memo defines a portion of the ManagementInformation Base (MIB) for use with networkmanagement protocols in TCP/IP-based Internets.In particular, it defines objects for managingversion 2 of the Open Shortest Path First RoutingProtocol. Version 2 of the OSPF protocol is specific to the IPv4 address family.

5.2 Applications

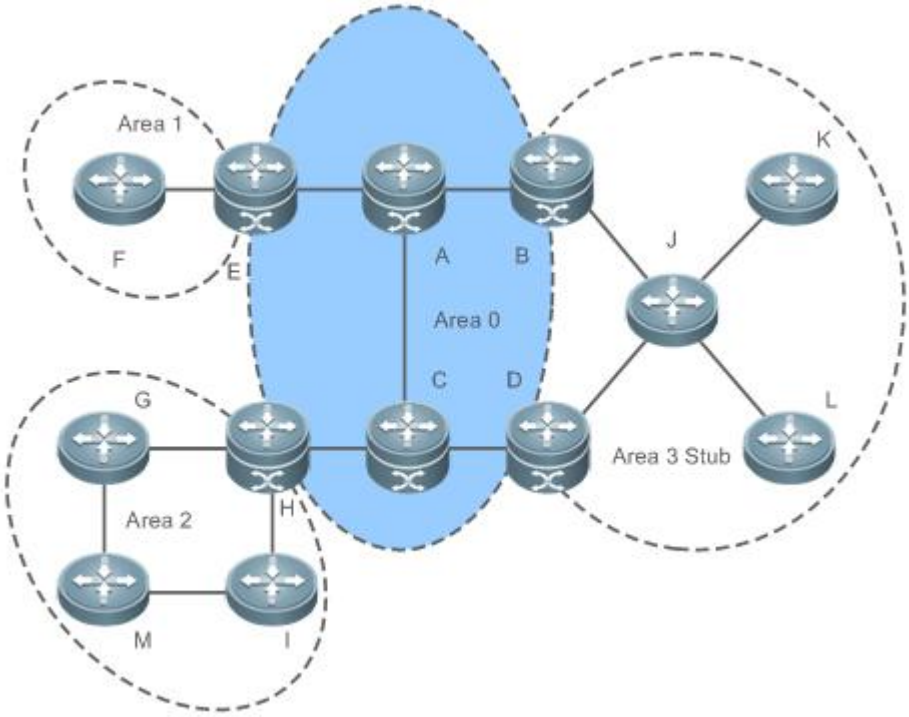
Application	Description
Intra-Domain Interworking	OSPF runs within the AS, which is divided into several areas.

5.2.1 Intra-Domain Interworking

Scenario

OSPF runs within the AS. If the number of routers exceeds 40, it is recommended that the AS be divided into several areas. Generally, high-end devices featuring reliable performance and fast processing speed are deployed in a backbone area, and low-end or medium-range devices with relatively lower performance can be deployed in a normal area. All normal areas must be connected to the backbone area. It is recommended that a normal arealocated on the stub be configured as a stub area. As shown in Figure 3- 5- 1, the network is divided into four areas. Communication between these areas must go through the backbone area, that is area 0.

Figure 3- 5- 1 Division of the OSPF Areas



Remarks	A, B, C, D, E, and H are located in the backbone area, and are backbone routers. Area 3 is configured as a stub area.

Deployment

- OSPF runs on all routers within the AS to implement unicast routing.

5.3 Features

Basic Concepts

Routing Domain

All routers in an AS must be interconnected and use the same routing protocol. Therefore, the AS is also called routing domain.

An AS on which OSPF runs is also called OSPF routing domain, or OSPF domain for short.

OSPF Process

OSPF supports multiple instances, and each instance corresponds to an OSPF process.

One or more OSPF processes can be started on a router. Each OSPF process runs OSPF independently, and the processes are mutually isolated.

The process ID takes effect only on the local router, and does not affect exchange of OSPF packets on adjacent interfaces.

RouterID

The router ID uniquely identifies a router in an OSPF domain. Router IDs of any two routers cannot be the same.

If multiple OSPF processes exist on a router, each OSPF process uses one router ID. Router IDs of any two OSPF processes cannot be the same.

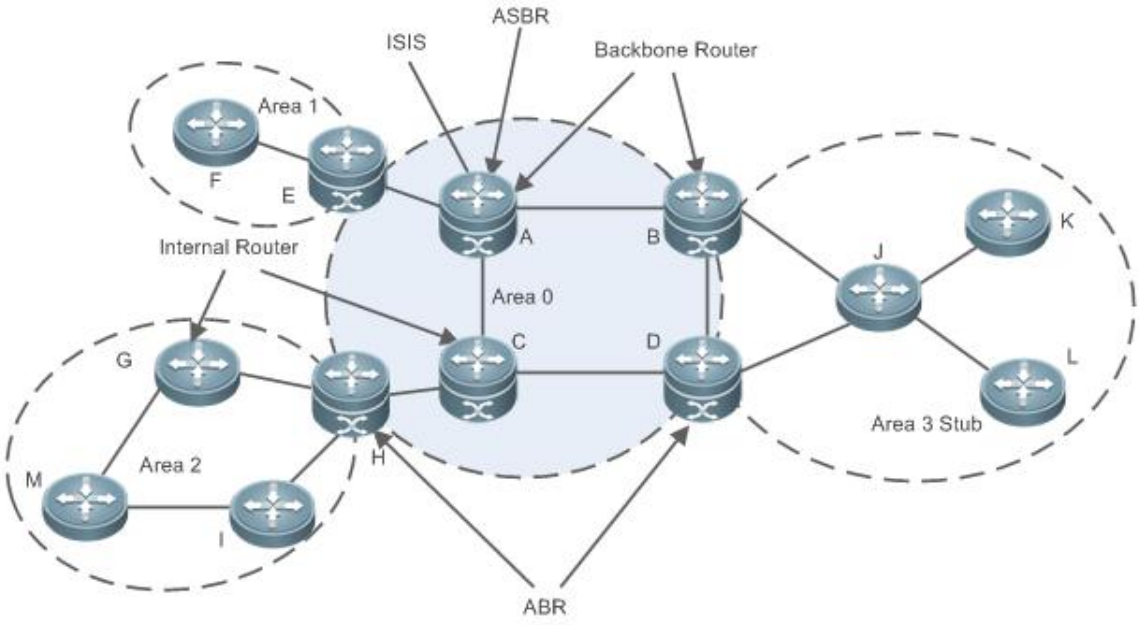
Area

OSPF supports multiple areas. An OSPF domain is divided into multiple areas to ease the computing pressure of a large-scale network.

An area is a logical group of routers, and each group is identified by an area ID. The border between areas is a router. A router may belong to one area or multiple areas. One network segment (link) can belong to only one area, or each OSPF-enabled interface must belong to a specified area.

Area 0 is the backbone area, and other areas are normal areas. Normal areas must be directly connected to the backbone area.

Figure 3- 2 Division of the OSPF Areas



OSPF Router

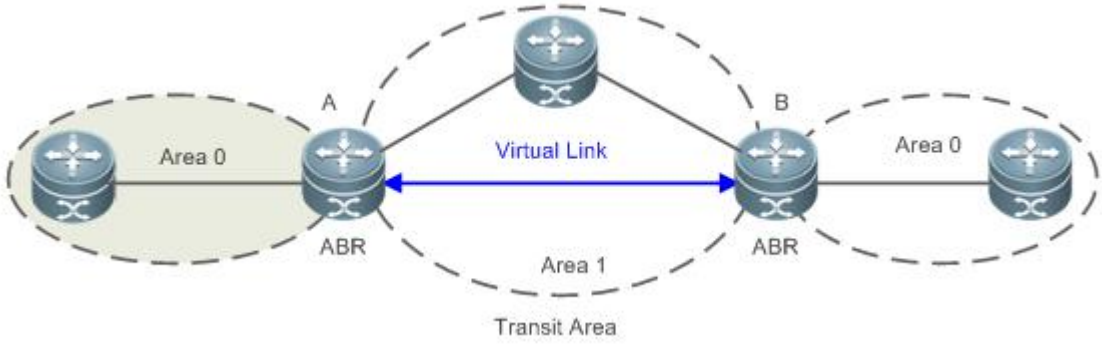
The following types of routers are defined in OSPF, and assigned with different responsibilities:

- Internal router
- All interface of an interval router belong to the same OSPF area. As shown in Figure 1-3, A, C, F, G, I, M, J, K, and L are internal routers.
- Area border router (ABR)
- An ABR is used to connect the backbone area with a normal area. An ABR belongs to two or more areas, and one of the areas must be the backbone area. As shown in Figure 1-3, B, D, E, and H are ABRs.
- Backbone router
- A backbone router has at least one interface that belongs to the backbone area. All ABRs and all routers in area 0 are backbone routers. As shown in Figure 3- , A, B, C, D, E, and H are backbone routers.
- AS boundary router (ASBR)
- An ASBR is used to exchange routing information with other ASs. An ASBR is not necessarily located on the border of an AS. It may be a router inside an area, or an ABR. As shown in Figure 1-3, A is an ASBR.

Virtual Link

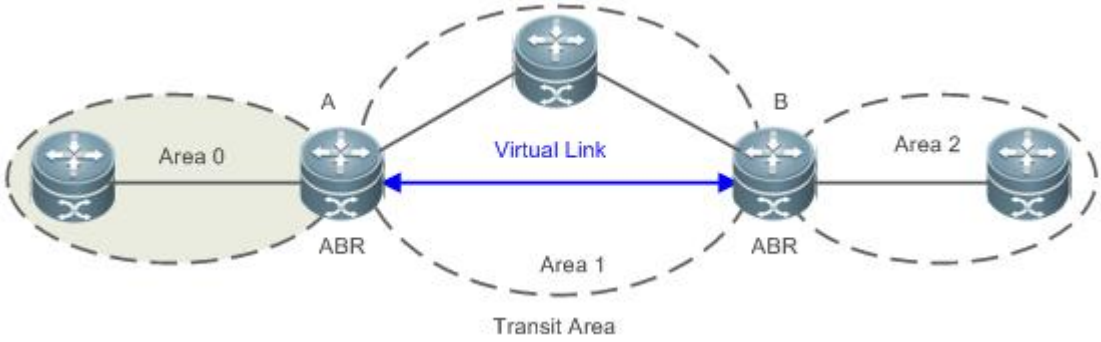
OSPF supports virtual links. A virtual link is a logical link that belongs to the backbone area. It is used to resolve the problems such as a discontinuous backbone area or a failure to directly connect a normal area to the backbone area on the physical network. A virtual link supports traversal of only one normal area, and this area is called transit area. Routers on both ends of a virtual link are ABRs.

Figure 5- 2Discontinuous Backbone Area on the Physical Network



As shown in Figure 5- 2, a virtual link is set up between A and B to connect two separated area 0s. Area 1 is a transit area, and A and B are ABRs of area 1.

Figure 5- 3Failure to Directly Connect a Normal Area to the Backbone Areaon the Physical Network



As shown in Figure 5- 2, a virtual link is set up between A and B to extend area 0 to B so that area 0 can be directly connected to area 2 on B. Area 1 is a transit area, A is an ABR of area 1, and B is an ABR of area 0 and area 2.

↘ LSA

OSPF describes the routing information by means of Link State Advertisement (LSA).

LSA Type	Description
Router-LSA(Type 1)	This LSA is originated by every router. It describes the link state and cost of the router, and is advertised only within the area where the originating router is located.
Network-LSA(Type 2)	This LSA is originated by a designated routers (DR) on the NBMA network. It describes the link state in the current network segment, and is advertised only within the area where the DR is located.
Network-summary-LSA(Type 3)	This LSA is originated by an ABR. It describes a route to another area, and is advertised to areas except totally stub areas or Not-So-Stubby Area (NSSA) areas.
ASBR-summary-LSA(Type 4)	This LSA is originated by an ABR. It describes a route to an ASBR, and is advertised to areas except areas where the ASBR is located.
AS-external-LSA(Type 5)	This LSA is originated by an ABR. It describes a route to a destination outside the AS, and is advertised to all areas except the stub and NSSA areas.
NSSA LSA(Type 7)	This LSA is originated by an ABR. It describes a route to a destination outside the AS, and is advertised only within the NASSA areas.
Opaque LSA(Type 9/Type 10/Type 11)	Opaque LSAs provide a generalized mechanism to allow for the future extensibility of OSPF, wherein, ● Type 9 LSAs are only advertised within the network segment where interfaces resides. The

LSA Type	Description
	Grace LSA used to support graceful restart (GR) is one of Type 9 LSAs. ● Type 10 LSAs are advertised within an area. The LSA used to support Traffic Engineering (TE) is one of Type 10 LSAs. ● Type 11 LSAs are advertised within an AS. At present, there are no application examples of Type 11 LSAs.

Stub areas, NSSA areas, totally stub areas, and totally NSSA areas are special forms of normal areas and help reduce the load of routers and enhance reliability of OSPF routes.

OSPF Packet

The following table lists the protocol packets used by OSPF. These OSPF packets are encapsulated in IP packets and transmitted in multicast or unicast mode.

Packet Type	Description
Hello	Hello packets are sent periodically to discover and maintain OSPF neighbor relationships.
Database Description (DD)	DD packets carry brief information about the local Link-State Database (LSDB) and are used to synchronize the LSDBs between OSPF neighbors.
Link State Request (LSR)	LSR packets are used to request the required LSAs from neighbors. LSR packets are sent only after DD packets are exchanged successfully between OSPF neighbors.
Link State Update (LSU)	LSU packets are used to send the required LSAs to peers.
Link State Acknowledgment (LSAck)	LSAck packets are used to acknowledge the received LSAs.

Overview

Feature	Description
Link-State Routing Protocols	Run OSPF on the router to obtain routes to different destinations on the network.
OSPF Route Management	Plan or optimize OSPF routes through manual configuration to implement management of OSPF routes.
Enhanced Security and Reliability	Use functions such as authentication to enhance security, stability, and reliability of OSPF.
Network Management	Use functions such as the management information base (MIB) and Syslog to facilitate OSPF management.

5.3.1 Link-State Routing Protocols

OSPF is a type of link-state routing protocols. Its working process is as follows:

- Neighbor discovery → Bidirectional communication
- An OSPF neighbor relationship is set up between adjacent routers, and bidirectional communication is maintained.
- Database synchronization → Full adjacency
- A router uses LSAs to advertise all its link states. LSAs are exchanged between neighbors and the link state database (LSDB) is synchronized to achieve full adjacency.
- Shortest Path Tree (SPT) computation → Formation of a routing table
- The router computes the shortest path to each destination network based on the LSDB and forms an OSPF routing table.

Working Principle

Neighbor Discovery → Bidirectional Communication

Routers send Hello packets through all OSPF-enabled interfaces (or virtual links). If Hello packets can be exchanged between two routers, and parameters carried in the Hello packets can be successfully negotiated, the two routers become neighbors. Routers that are mutually neighbors find their own router IDs from Hello packets sent from neighbors, and bidirectional communication is set up.

A Hello packet includes, but is not limited to, the following information:

- Router ID of the originating router
- Area ID of the originating router interface (or virtual link)
- Subnet mask of the originating router interface (or virtual link)
- Authentication information of the originating router interface (or virtual link)
- Hello interval of the originating router interface (or virtual link)
- Neighbor dead interval of the originating router interface (or virtual link)
- Priority of the originating router interface (used for DR/BDR election)
- IP addresses of the DR and Backup Designated Router (BDR)
- Router ID of the neighbor of the originating router

Database Synchronization → Full Adjacency

After bidirectional communication is set up between neighbor routers, the DD, LSR, LSU, and LSAck packets are used to exchange LSAs and set up the adjacency. The brief process is as follows:

- A router generates an LSA to describe all link states on the router.
- The LSA is exchanged between neighbors. When a router receives the LSA from its neighbor, it copies the LSA and saves the copy in the local LSDB, and then advertises the LSA to other neighbors.
- When the router and its neighbors obtain the same LSDB, full adjacency is achieved.

OSPF will be very quiet without changes in link costs or network addition or deletion. If any change takes place, the changed link states are advertised to quickly synchronize the LSDB.

SPT Computation → Formation of a Routing Table

After the complete LSDB is obtained from the router, the Dijkstra algorithm is run to generate an SPT from the local router to each destination network. The SPT records the destination networks, next-hop addresses, and costs. OSPF generates a routing table based on the SPT.

If changes in link costs or network addition or deletion take place, the LSDB will be updated. The router again runs the Dijkstra algorithm, generates a new SPT, and updates the routing table.

The Dijkstra algorithm is used to find a shortest path from a vertex to other vertices in a weighted directed graph.

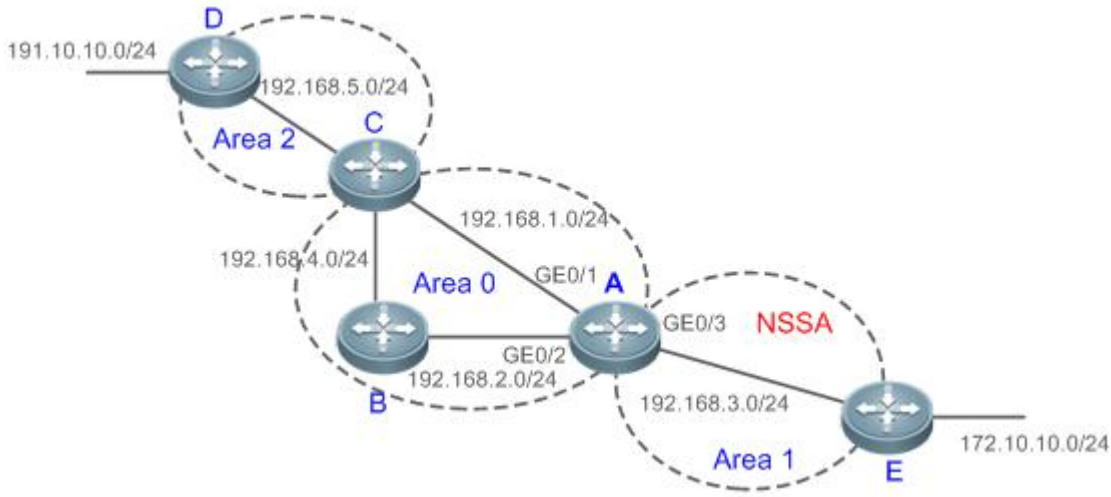
OSPF Network Types

A router does not necessarily need to exchange LSAs with every neighbor and set upan adjacency with every neighbor. To improve efficiency, OSPF classifies networks that use various link layer protocols into five types so that LSAs are exchanged in different ways to set upan adjacency:

- Broadcast
- Neighbors are discovered, and the DR and BDR are elected.
- The DR (or BDR) exchanges LSAs with all other routers to set up an adjacency. Except the DR and BDR, all other routers do not exchange LSAs with each other, and the adjacency is not set up.
- Ethernet and fiber distributed data interface (FDDI) belong to the broadcast network type by default.
- Non-broadcast multiple access (NBMA)
- Neighbors are manually configured, and the DR and BDR are elected.
- The DR (or BDR) exchanges LSAs with all other routers to set up an adjacency. Except the DR and BDR, all other routers do not exchange LSAs with each other, and the adjacency is not set up.
- X.25, frame relay, and ATM belong to NBMA networks by default.
- Point-to-point (P2P)
- Neighbors are automatically discovered, and the DR or BDR is not elected.
- LSAs are exchanged between routers at both ends of the link, and the adjacency is set up.
- PPP,HDLC, and LAPB belongs to the P2P network type by default.
- Point-to-multipoint (P2MP)
- Neighbors are automatically discovered, and the DR or BDR is not elected.
- LSAs are exchanged between any two routers, and the adjacency is set up.
- Networks without any link layer protocol belong to the P2MP network type by default. P2MP broadcast
- Neighbors are manually configured, and the DR or BDR is not elected.
- LSAs are exchanged between any two routers, and the adjacency is set up.
- Networks without any link layer protocol belong to the P2MP network type by default.

OSPF Route Types

Figure 5- 4



Display the OSPF routes (marked in red) in the routing table of Router A.

```
A#show ip route

Codes:    C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
O N2 172.10.10.0/24 [110/20] via 192.168.3.2, 00:01:00,GigabitEthernet 0/3
O E2 191.10.10.0/24 [110/20] via 192.168.1.2, 01:11:26,GigabitEthernet 0/1
C       192.168.1.0/24 is directly connected,GigabitEthernet 0/1
C       192.168.1.1/32 is local host.
C       192.168.2.0/24 is directly connected,GigabitEthernet 0/2
C       192.168.2.1/32 is local host.
C       192.168.3.0/24 is directly connected,GigabitEthernet 0/3
C       192.168.3.1/32 is local host.
O       192.168.4.0/24 [110/2] via 192.168.2.2, 00:00:02,GigabitEthernet 0/2
O IA 192.168.5.0/24 [110/3] via 192.168.1.2, 00:01:02,GigabitEthernet 0/1
```

A mark is displayed in front of each OSPF route to indicate the type of the route. There are six types of OSPF routes:

- O: Intra-area route
- This type of route describes how to arrive ata destination network in the local area. The cost of this type of route is equal to the cost of the route from the local router to the destination network.
- IA: Inter-area route
- This type of route describes how to arrive at a destination network in another area. The cost of this type of route is equal to the cost of the route from the local router to the destination network.
- E1: Type 1 external route
- This type of route describes how to arrive at a destination network outside the AS. The cost of this type of route is equal to the cost of the route from the local router to the ASBR plus the cost of the route from the ASBR to the destination network. This type of route does not exist on routers in the stub or NSSA area.
- E2: Type 2 external route
- This type of route describes how to arrive at a destination network outside the AS. The cost of this type of route is equal to the cost of the route from the ASBR to the destination network. This type of route does not exist on routers in the stub or NSSA area.
- N1: Type 1 external route of the NSSA area

- This type of route describes how to arrive at a destination network outside the AS through the ASBR in the NSSA area. The cost of this type of route is equal to the cost of the route from the local router to the ASBR plus the cost of the route from the ASBR to the destination network. This type of route exists only on routers in the NSSA area.
- N2: Type 2 external route of the NSSA area
- This type of route describes how to arrive at a destination network outside the AS through the ASBR in the NSSA area. The cost of this type of route is equal to the cost of the route from the ASBR to the destination network. This type of route exists only on routers in the NSSA area.

Reliability of E2 and N2 routes is poor. OSPF believes that the cost of the route from the ASBR to a destination outside an AS is far greater than the cost of the route to the ASBR within the AS. Therefore, when the route cost is computed, only the cost of the route from the ASBR to a destination outside an AS is considered.

Related Configuration

Enabling OSPF

OSPF is disabled by default.

Run the **router ospf** 1 command to create an OSPF process on the router.

Run the **network area** command to enable OSPF on the interface and specify the area ID.

Run the **area virtual-link** command to create a virtual link on the router. The virtual link can be treated as a logical interface.

Router ID

By default, the OSPF process elects the largest IP address among the IP addresses of all the loopback interfaces as the router ID. If the loopback interfaces configured with IP addresses are not available, the OSPF process elects the largest IP address among the IP addresses of all the loopback interfaces as the router ID.

Alternatively, you can run the **router-id** command to manually specify the router ID.

Protocol Control Parameters

Run the **ip ospf hello-interval** command to modify the Hello interval on the interface. The default value is 10s (or 30s for NBMA networks).

Run the **ip ospf dead-interval** command to modify the neighbor dead interval on the interface. The default value is four times the Hello interval.

Use the **poll-interval** parameter in the **neighbor** command to modify the neighbor polling interval on the NBMA interface. The default value is 120s.

Run the **ip ospf transmit-delay** command to modify the LSU packet transmission delay on the interface. The default value is 1s.

Run the **ip ospf retransmit-interval** command to modify the LSU packet retransmission interval on the interface. The default value is 5s.

Use the **hello-interval** parameter in the **area virtual-link**command to modify the Hello interval on the virtual link. The default value is 10s.

Use the **dead-interval** parameter in the **area virtual-link**command to modify the neighbor dead interval on the virtual link. The default value is four times the Hello interval.

Use the **transmit-delay** parameter in the **area virtual-link**command to modify the LSU packet transmission delay on the virtual link. The default value is 1s.

Use the **retransmit-interval** parameter in the **area virtual-link**command to modify the LSU packet retransmission interval on the virtual link. The default value is 5s.

Run the **timers throttle lsa all** command to modify parameters of the exponential backoff algorithm that generates LSAs. The default values of these parameters are 0 ms, 5000 ms, and 5000 ms.

Run the **timerspacinglsa-group** command to modify the LSA group update interval. The default value is 30s.

Run the **timers pacing lsa-transmit** command to modify the LS-UPD packet sending interval and the number of sent LS-UPD packets. The default values are 40 ms and 1.

Run the **timers lsa arrival** command to modify the delay after which the same LSA is received. The default value is 1000 ms.

Run the **timers throttle spf** command to modify the SPT computation delay, minimum interval between two SPT computations, and maximum interval between two SPT computations. The default values are 1000 ms, 5000 ms, and 10000 ms.

↘ OSPF Network Types

By default, Ethernet and FDDI belong to the broadcast type, X.25, frame relay, and ATM belong to the NBMA type, and PPP, HDLC, and LAPB belong to the P2P type.

Run the **ip ospf network** command to manually specify the network type of an interface.

Run the **neighbor** command to manually specify a neighbor. For the NBMA and P2MP non-broadcast types, you must manually specify neighbors.

Run the **ip ospf priority** command to adjust the priorities of interfaces, which are used for DR/BDR election. The DR/BDR election is required for the broadcast and NBMA types. The router with the highest priority wins in the election, and the router with the priority of 0 does not participate in the election. The default value is 1.

5.3.2 OSPF Route Management

Plan or optimize OSPF routes through manual configuration to implement management of OSPF routes.

Working Principle

↘ (Totally) Stub Area and (Totally)NSSA Area

The (totally) stub and (totally)NSSA areas help reduce the protocol interaction load and the size of the routing table.

- If an appropriate area is configured as a (totally) stub or NSSA area, advertisement of a large number of Type 5 and Type 3 LSAs can be avoided within the area.

Area	Type1 and Type2 LSAs	Type 3 LSA	Type 4 LSA	Type 5 LSA	Type 7 LSA
Non (totally) stub area and NSSA area	Allowed	Allowed	Allowed	Allowed	Not allowed
Stub area	Allowed	Allowed (containing one default route)	Not allowed	Not allowed	Not allowed
Totally stub area	Allowed	Only one default route is allowed.	Not allowed	Not allowed	Not allowed
NSSA area	Allowed	Allowed (containing one default route)	Allowed	Not allowed	Allowed
Totally NSSA area	Allowed	Only one default route is	Allowed	Not allowed	Allowed

		allowed.			

- The ABR uses Type 3LSAs to advertise a default route to the (totally) stub or NSSA area.
- The ABR converts Type 7 LSAs in the totally NSSA area to Type 5LSAs, and advertise Type5LSAs to the backbone area.
- If an area is appropriately configured as a (totally) stub area or an NSSA area, a large number of E1, E2, and IA routes will not be added to the routing table of a router in the area.

Area	Routes Available in the Routing Table of a Router Inside the Area
Non (totally) stub area and NSSA area	O: a route to a destination network in the local area IA: a route to a destination network in another area E1 or E2: a route or default route to a destination network segment outside the AS (via any ASBR in the AS)
Stub area	O: a route to a destination network in the local area IA: a route or a default route to a destination network in another area
Totally stub area	O: a route to a destination network in the local area IA: a default route
NSSA area	O: a route to a destination network in the local area IA: a route or a default route to a destination network in another area N1 or N2: a route or default route to a destination network segment outside the AS (via any ASBR in the local area)
Totally NSSA area	O: a route to a destination network in the local area IA: a default route N1 or N2: a route or default route to a destination network segment outside the AS (via any ASBR in the local area)

Route Redistribution

Route redistribution refers to the process of introducing routes of other routing protocols, routes of other OSPF processes, static routes, and direct routes that exist on the device to an OSPF process so that these routes can be advertised to neighbors using Type 5 and Type 7 LSAs. A default route cannot be introduced during route redistribution.

Route redistribution is often used for interworking between ASs. You can configure route redistribution on an ASBR to advertise routes outside an AS to the interior of the AS, or routes inside an AS to the exterior of the AS.

Default Route Introduction

By configuring a command on an ASBR, you can introduce a default route to an OSPF process so that the route can be advertised to neighbors using Type 5 and Type 7 LSAs.

Default route introduction is often used for interworking between ASs. One default route is used to replace all the routes outside an AS.

Route Summarization

Route summarization is a process of summarizing routing information with the same prefix into one route, and advertising the summarized route (replacing a large number of individual routes) to neighbors. Route summarization helps reduce the protocol interaction load and the size of the routing table.

By default, the ABR advertises inter-area routing information by using Type3 LSAs within a network segment, and advertises redistributed routing information by using Type 5 and Type 7 LSAs.If continuous network segments exist, it is recommended that you configure route summarization.

When configuring route summarization, the summarization range may exceed the actual network scope of routes. If data is sent to a network beyond the summarization range, a routing loop may be formed and the router processing load may increase.To prevent these problems, the ABR or ASBR automatically adds a discard route to the routing table. This route will not be advertised.

Route Filtering

OSPF supports route filtering to ensure security and facilitate control when the routing information is being learned, exchanged, or used.

Using configuration commands, you can configure route filtering for the following items:

- Interface: The interface is prevented from sending routing information (any LSAs) or exchanging routing information (any LSAs) with neighbors.
- Routing information advertised between areas: Only the routing information that meets the filtering conditions can be advertised to another area (Type 3 LSAs).
- Routing information outside an AS: Only the routing information that meets the filtering conditions can be redistributed to the OSPF process(Type 5 and Type 7 LSAs).
- LSAs received by a router: In the OSPF routing table, only the routes that are computed based on the LSAs meeting the filtering conditions can be advertised.

Route Cost

If redundancy links or devices exist on the network, multiple paths may exist from the local device to the destination network. OSPF selects the path with the minimum total cost to form an OSPF route. The total cost of a path is equal to the sum of the costs of individual links along the path.The total cost of a path can be minimized by modifying the costs of individual links along the path. In this way, OSPF selects this path to form a route.

Using configuration commands, you can modify the link costs:

- Cost from an interface to a directly connected network segment and cost from the interface to a neighbor
- Costfrom an ABR to the inter-area summarization network segment and cost from the ABR to the default network segment
- Costfrom an ASBR to an external network segment and cost from the ASBR to the default network segment

Both the cost and the metric indicate the cost and are not differentiated from each other.

OSPF Administrative Distance

The administrative distance (AD) evaluates reliability of a route, and the value is an integer ranging from 0 to 255. A smaller AD value indicates that the route is more trustworthy. If multiples exist to the same destination, the route preferentially selects a route with a smaller AD value. The route with a greater AD value becomes a floating route, that is, a standby route of the optimum route.

By default, the route coming from one source corresponds to an AD value. The AD value is a local concept. Modifying the AD value affects route selection only on the current router.

Route Source	Directly-Connected Network	Static Route	OSPF Route	RIP Route	Unreachable Route

Default AD	0	1	110	120	255

Related Configuration

Stub Area and NSSA Area

No stub or NSSA area is configured by default.

Run the **area stub** command to configure a specified area as a stub area.

Run the **area nssa** command to configure a specified area as an NSSA area.

- The backbone area cannot be configured as a stub or an NSSA area.
- A transit area (with virtual links going through) cannot be configured as a stub or an NSSA area.
- An area containing an ASBR cannot be configured as a stub area.

Route Redistribution and Default Route Introduction

By default, routes are not redistributed and the default route is not introduced.

Run the **redistribute** command to configure route redistribution.

Run the **default-information originate** command to introduce the default route.

After configuring route redistribution and default route introduction, the route automatically becomes an ASBR.

Route Summarization

By default, routes are not summarized. If route summarization is configured, a discard route will be automatically added.

Run the **arearange** command to summarize routes distributed between areas (Type 3 LSA) on the ABR.

Run the **summary-address** command to summarize redistributed routes (Type 5 and Type 7 LSAs) on the ASBR.

Run the **discard-route** command to add a discard route to the routing table.

Route Filtering

By default, routes are not filtered.

Run the **passive-interface** command to configure a passive interface. Routing information (any LSAs) cannot be exchanged on a passive interface.

Run the **ip ospfdatabase-filter all out** command to prohibit an interface from sending routing information (any LSAs).

Run the **area filter-list** command to filter routing information advertised between areas on the ABR. Only the routing information that meets the filtering conditions can be advertised to another area (Type 3 LSAs).

Use the **route-map** parameter in the **redistribute** command, or use the **distribute-list out** command to filter the external routing information of the AS on the ASBR. Only the routing information that meets the filtering conditions can be redistributed to the OSPF process (Type 5 and Type 7 LSAs).

Run the **distribute-list in** command to filter LSAs received by the router. In the OSPF routing table, only the routes that are computed based on the LSAs meeting the filtering conditions can be advertised.

Route Cost

- Cost from the interface to the directly-connected network segment (cost on the interface)
- The default value is the auto cost. Auto cost = Reference bandwidth/Interface bandwidth
- Run the **auto-cost reference-bandwidth** command to set the reference bandwidth of auto cost. The default value is 100 Mbps.
- Run the **ip ospf cost** command to manually set the cost of the interface. The configuration priority of this item is higher than that of the auto cost.
- Cost from the interface to a specified neighbor (that is, cost from the local device to a specified neighbor)
- The default value is the auto cost.
- Use the **cost** parameter in the **neighbor** command to modify the cost from the interface to a specified neighbor. The configuration priority of this item is higher than that of the cost of the interface.
- This configuration item is applicable only to P2MP-type interfaces.
- Cost from the ABR to the inter-area summarization network segment (that is, the cost of the summarized inter-area route)
- If OSPF routing is compatible with RFC1583, the default value is the minimum cost among all costs of the summarized links; otherwise, the default value is the maximum cost among all costs of the summarized links.
- Run the **compatible rfc1583** command to make OSPF routing compatible with RFC1583. By default, OSPF routing is compatible with RFC1583.
- Use the **cost** parameter in the **area range** command to modify the cost of inter-area route summarization.
- Cost from the ABR to the default network segment (that is, the cost of the default route that is automatically advertised by the ABR to the stub or NSSA areas)
- The default value is 1.
- Run the **area default-cost** command to modify the cost of the default route that the ABR automatically advertise to the stub or NSSA areas.
- Cost from the ASBR to an external network segment (that is, the metric of an external route)
- By default, the metric of other types of redistributed routes is 20, and the route type is Type 2 External.
- Run the **default-metric** command to modify the default metric of the external route.
- Use the **metric**,**metric-type** and **route-map** parameters in the **redistribute** command to modify the metric and route type of the external route.
- Cost from the ASBR to the default network segment (that is, the metric of the default route that is manually introduced)
- By default, the metric is 1, and the route type is Type 2 External.
- Use the **metric**,**metric-type** and **route-map** parameters in the **default-information originate** command to modify the metric and route type of the default route that is manually introduced.
- Use the **metric** and **metric-type** parametersof**default-information originate**in the **area nssa** command to modify the metric and type of the default route that is manually introduced to the NSSA area.
- Run the **max-metric router-lsa** command to set metrics of all routes advertised on the router to the maximum value. In this way, the total cost of any path that passes through this router will become very large, and the path can hardly become the shortest path.

OSPF Administrative Distance

By default, the OSPF AD is 110.

Run the **distance** command to set the AD of an OSPF route.

5.3.3 Enhanced Security and Reliability

Use functions such as authentication to enhance security, stability, and reliability of OSPF.

Working Principle

- **Authentication**

Authentication prevents routers that illegally access the network and hosts that forge OSPF packet from participating in the OSPF process. OSPF packets received on the OSPF interface (or at both ends of the virtual link) are authenticated. If authentication fails, the packets are discarded and the adjacency cannot be set up.

Enabling authentication can avoid learning unauthenticated or invalid routes, thus preventing advertising valid routes to unauthenticated devices. In the broadcast-type network, authentication also prevents unauthenticated devices from becoming designated devices, ensuring stability of the routing system and protecting the routing system against intrusions.

- **MTU Verification**

On receiving a DD packet, OSPF checks whether the MTU of the neighbor interface is the same as the MTU of the local interface. If the MTU of the interface specified in the received DD packet is greater than the MTU of the interface that receives the packet, the adjacency cannot be set up. Disabling MTU verification can avoid this problem.

- **Source Address Verification**

Generally, the source address of a packet received by OSPF is in the same network segment as the receiving interface. The addresses at both ends of a P2P link are configured separately and are not necessarily in the same network segment. In this scenario, as the peer address information will be notified during the P2P link negotiation process, OSPF checks whether the source address of the packet is the address advertised by the peer during negotiation. If not, OSPF determines that the packet is invalid and discards this packet. In particular, OSPF does not verify the address of an unnumbered interface.

In some scenarios, the source address of a packet received by OSPF maynot be in the same network segment as the receiving interface, and therefore OSPF address verification fails. For example, the negotiated peer address cannot be obtained on a P2P link. In this scenario, source address verification must be disabled to ensure that the OSPF adjacency can be properly set up.

- **Two-Way Maintenance**

OSPF routers periodically send Hello packets to each other to maintain the adjacency. On a large network, a lot of packets may be sent or received, occupying too much CPU and memory. As a result, some packets are delayed or discarded. If the processing time of Hello packets exceeds the dead interval, the adjacency will be destroyed.

If the two-way maintenance function is enabled, in addition to the Hello packets, the DD, LSU, LSR, and LSAck packets can also be used to maintain the bidirectional communication between neighbors, which makes the adjacency more stable.

- **Concurrent Neighbor Interaction Restriction**

When a router simultaneously exchanges data with multiple neighbors, its performance may be affected. If the maximum number of neighbors that concurrently initiate or accept interaction with the OSPF process, the router can interact with neighbors by batches, which ensures data forwarding and other key services.

Overflow

OSPF requires that routers in the same area store the same LSDB. The number of routers keeps increasing on the network. Some routers, however, cannot store so much routing information due to the limited system resources. The large amount of routing information may exhaust the system resources of routers, causing failures of the routers.

The overflow function limit the number of external routes in the LSDB to control the size of the LSDB.

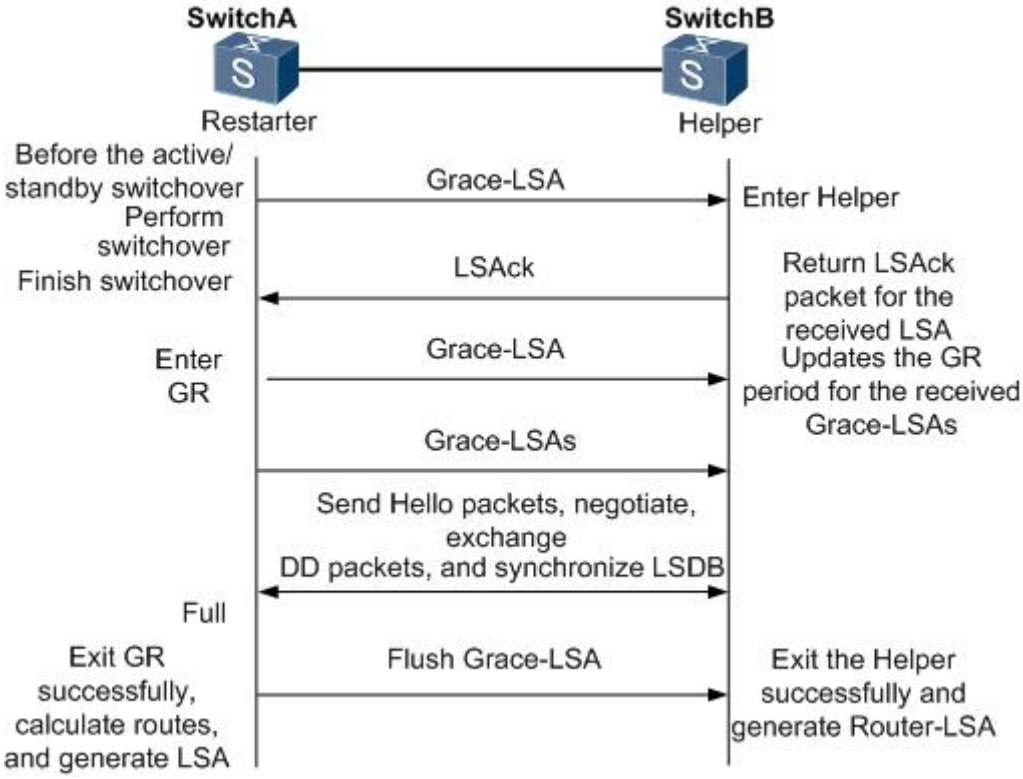
When the number of external routes on a router exceeds the upper limit, the router enters the overflow state. The router deletes the external routes generated by itself from the LSDB, and does not generate new external routes. In addition, the router discards the newly received external routes. After the overflow state timer (5s) expires, if the number of external routes is lower than the upper limit, the normal state is restored.

GR

The control and forwarding separated technology is widely used among routers. On a relatively stable network topology, when a GR-enabled router is restarted on the control plane, data forwarding can continue on the forwarding plane. In addition, actions (such as adjacency re-forming and route computation) performed on the control plane do not affect functions of the forwarding plane. In this way, service interruption caused by route flapping can be avoided, thus enhancing reliability of the entire network.

Currently, the GR function is used only during active/standby switchover and system upgrade.

Figure 5- 5Normal OSPF GR Process



- The GR process requires collaboration between the restarter and the helper. The restarter is the router where GR occurs. The helper is a neighbor of the restarter.
- When entering or exiting the GR process, the restarter sends a Grace-LSA to the neighbor, notifying the neighbor to enter or exit the helper state.

- When the adjacency between the restarter and the helper reaches the Full state, the router can exit the GR process successfully.

5.4 Configuration

Configuration	Description and Command	
Configuring OSPF Basic Functions	(Mandatory) It is used to build an OSPF routing domain.	
	routerospf	Creates an OSPF process.
	router-id	Configures a router ID.
	network area	Enables OSPF on an interface and specifies an area ID.
	area virtual-link	Creates a virtual link.
Setting the Network Type	(Optional) The configurations are mandatory if the physical network is the X.25, frame relay, or ATM network.	
	ip ospf network	Defines the network type.
	neighbor	Specifies a neighbor.
	ip ospf priority	Configures the DR priority.
Configuring Route Redistribution and Default Route	(Optional) The configurations are recommended if the OSPF routing domain is connected with an external network.	
	redistribute	Configures route redistribution.
	default-information originate	Introduces a default route.
Configuring Stub Area and NSSA Area	(Optional) It is used to reduce interaction of routing information and the size of routing table, and enhance stability of routes.	
	areastub	Configures a stub area.
	areanssa	Configures an NSSA area.
Configuring Route Summarization	(Optional) It is used to reduce interaction of routing information and the size of routing table, and enhance stability of routes.	
	arearange	Summarizes routes that are advertised between areas.
	summary-address	Summarizes routes that are introduced through redistribution.
	discard-route	Adds a discard route to the routing table.
Configuring Route Filtering	(Optional) It is used to manually control interaction of routing information and filter available OSPF routes.	
	passive-interface	Configures a passive interface.
	ip ospfdatabase-filter all out	Prohibits an interface from sending LSAs.
	area filter-list	Filters routes that are advertised between areas..
	distribute-list out	Filters routes that are introduced through redistribution.
	distribute-listin	Filters routes that are calculated based on the received LSAs.

Configuration	Description and Command	
Modifying Route Cost and AD	(Optional) It is used to manually control the shortest route computed by OSPF and determine whether to select an OSPF route preferentially.	
	auto-cost reference-bandwidth	Modifies the reference bandwidth of the auto cost.
	ip ospf cost	Modifies the cost in the outbound direction of an interface.
	areadefault-cost	Modifies the cost of the default route in a stub or an NSSA area.
	default-metric	Modifies the default metric of a redistributed route.
	max-metric router-lsa	Configures the maximum metric.
	compatible rfc1583	Enables the routing rules to be compatible with RFC1583.
	distance	Modifies the OSPF AD.
Enabling Authentication	(Optional) It is used to prevent routers that illegally access the network and hosts that forge OSPF packets from participating in the OSPF protocol process.	
	areaauthentication	Enables authentication and sets the authentication mode in an area.
	ip ospf authentication	Enables authentication and sets the authentication mode on an interface.
	ip ospf authentication-key	Sets the text authentication key on an interface.
	ip ospfmessage-digest-keymd5	Sets the MD5 authentication key on an interface.
Enabling Overflow	(Optional) It is used to prevent the problem that OSPF processes stop running due to over-consumption of the memory.	
	overflow memory-lack	Allows the router to enter the overflow state when the memory is insufficient.
	overflow database	Allows the router to enter the overflow state when the number of LSAs exceeds the preset limit.
	overflow database external	Allows the router to enter the overflow state when the number of external LSAs exceeds the preset limit.
Modifying the Maximum Number of Concurrent Neighbors	(Optional) It is used to prevent the problem of performance deterioration caused by over-consumption of the CPU.	
	max-concurrent-dd	Modifies the maximum number of con current neighbors on the current OSPF process.
	router ospf max-concurrent-dd	Modifies the maximum number of con current neighbors on all OSPF processes.

Configuration	Description and Command	
Disabling Source Address Verification	(Optional) It is used to prevent the problem that the adjacency cannot be set up due to the failure to obtain the peer address.	
	ip ospf source-check-ignore	Disables source address verification on an interface.
Disabling MTU Verification	(Optional) It is used to prevent the problem that the adjacency cannot be set up due to MTU inconsistency on the neighbor interface.	
	ip ospf mtu-ignore	Disables MTU verification on an interface.
Enabling Two-Way Maintenance	(Optional) It is used to prevent termination of the adjacencydue to the delay or loss of Hello packets.	
	two-way-maintain	Enables two-way maintenance.
Enabling GR	(Optional) It is used to retain OSPF routing forwarding during restart or active/standby switchover of the OSPF processes to prevent traffic interruption.	
	graceful-restart	Configures the restarter function.
	graceful-restart helper	Configures the helper function.
Enabling the Fast Hello Function	(Optional) It is used to quickly discover the death of a neighbor to prevent traffic interruption when a link is faulty.	
	ip ospf dead-intervalminimal hello-multiplier	Enabling the Fast Hello function on an interface.
Configuring the Network Management Function	(Optional) The configurations enable users to use the SNMP network management software to manage OSPF.	
	enable mib-binding	Binds the MIB with the current OSPF process.
	enable traps	Enables a specified trap for an OSPF process.
	snmp-server enable traps ospf	Allows the device to send OSPF traps.
	log-adj-changes	Allows the Syslog to record the adjacency changes.
Modifying Protocol Control Parameters	(Optional) You are advised not to modify protocol control parameters unless necessary.	
	ip ospf hello-interval	Modifies the Hello interval.
	ip ospf dead-interval	Modifies the neighbor death interval.
	timers throttle lsa all	Modifies parameters of the exponential backoff algorithm that generates LSAs.
	timers throttle route inter-area	Modifies the inter-area route computation delay.
	timers throttle route ase	Modifies the external route computation delay.
	timerspacinglsa-group	Modifies the LSA group update interval.
	timers pacing lsa-transmit	Modifies the LS-UPD packet sending interval.
	ip ospf transmit-delay	Modifies the LSU packet transmission delay.
	ip ospf retransmit-interval	Modifies the LSU packet retransmission interval.
	timers lsa arrival	Modifies the delay after which the same LSA is received.
	timers throttlespf	Modifies the SPT computation timer.

5.4.1 Configuring OSPF Basic Functions

Configuration Effect

- Set up an OSPF routing domain on the network to provide IPv4 unicast routing service for users on the network.

Notes

- Ensure that the IP unitcast routing function is enabled, that is, **ip routing** is not disabled; otherwise, OSPF cannot be enabled.
- It is strongly recommended that you manually configure the router ID.
- After **ip ospf disable all** is configured, the interface neither sends or receives any OSPF packet, nor participates in OSPF computation even if the interface belongs to the network.

Configuration Steps

Creating an OSPF Process

- Mandatory.
- The configuration is mandatory for every router.

Configuring a Router ID

- (Optional) It is strongly recommended that you manually configure the router ID.
- If the router ID is not configured, OSPF selects an interface IP address. If the IP address is not configured for any interface, or the configured IP addresses have been used by other OSPF instances, you must manually configure the router ID.

Enabling OSPF on an Interface and Specifying an Area ID

- Mandatory.
- The configuration is mandatory for every router.

Verification

- Run the **show ip route ospf** command to verify that the entries of the OSPF routing table are correctly loaded.
- Run the **ping** command to verify that the IPv4 unicast service is correctly configured.

Related Commands

Creating an OSPF Process

Command	**router ospf** *process-id* [**vrf** *vrf-name*]
Parameter Description	*process-id:* Indicates the OSPF process ID. If the process ID is not specified, the process ID is 1. *vrf-name:* Specifies the VPN routing and forwarding (VRF) to which the OSPF process belongs.
Command Mode	Global configuration mode
Usage Guide	Different OSPF processes are independent of each other, and can be treated as different routing protocols that run independently.

Configuring a Router ID

Command	**router-id***router-id*

Parameter Description	*router-id:* Indicates the router ID to be configured. It is expressed in the IP address.
Command Mode	OSPF routing process configuration mode
Usage Guide	Different OSPF processes are independent of each other, and can be treated as different routing protocols that run independently. Each OSPF process uses a unique router ID.

Enabling OSPF on an Interface and Specifying an Area ID

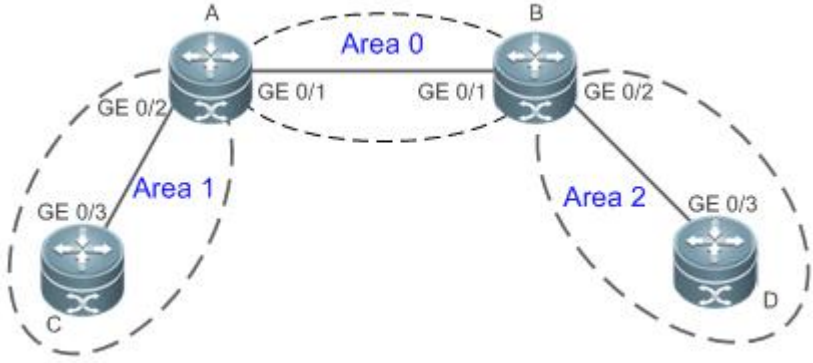
Command	**network** *ip-address wildcard* **area** *area-id*
Parameter Description	*ip-address*: Indicates the IP address of the interface. *wildcard:* Indicates the IP address comparison mode. **0** indicates accurate matching, and **1** indicates that no comparison is performed. *area-id:* Indicates the ID of an OSPF area. An OSPF area is always associated with an address range. To facilitate management, you can use a subnet as the ID of an OSPF area.
Command Mode	OSPF routing process configuration mode
Usage Guide	By defining *ip-address* and *wildcard*, you can use one command to associate multiple interfaces with one OSPF area. To run OSPF on one interface, you must include the primary IP address of the interface in the IP address range defined by **network area**. If the IP address range defined by **network area** contains only the secondary IP address of the interface, OSPF does not run on this interface. If the interface address matches the IP address ranges defined in the **network** commands of multiple OSPF processes, the OSPF process that the interface is associated with is determined based on the best match method.

Creating a Virtual Link

Command	**area** *area-id* **virtual-link** *router-id* [**authentication** [**message-digest** | **null**]] [**dead-interval**{ *seconds* | **minimal hello-multiplier** *multiplier*}] [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [[**authentication-key**[**0** |**7**] *key*] | [**message-digest-key** *key-id* **md5**[**0** |**7**] *key*]]
Parameter Description	*area-id:* Indicates the ID of the OSPF transit area. The area ID can be a decimal integer or an IP address. *router-id:* Indicates the ID of a neighborrouter on the virtual link. **dead-interval** *seconds:* Indicates the time that the neighbor is declared lost. The unit is second. The value ranges from 0 to 2,147,483,647. The setting of this parameter must be consistent with that on a neighbor. **minimal:** Indicates that the Fast Hello function is enabled to set the dead interval to 1s. **hello-multiplier:** Indicates the result of the dead interval multiple by the Hello interval in the Fast Hello function. *multiplier:* Indicates the number of Hello packets sent per second in the Fast Hello function. The value ranges from 3 to 20. **hello-interval** *seconds:* Indicates the interval at which OSPF sends the Hello packet to the virtual link. The unit is second. The value ranges from 1 to 65,535. The setting of this parameter must be consistent with that on a neighbor. **retransmit-interval** *seconds:* Indicates the OSPF LSA retransmission time. The unit is second. The value ranges from 1 to 65,535. **transmit-delay** *seconds:* Indicates the delay after which OSPF sends the LSA. The unit is second. The value ranges from 1 to 65,535. **authentication-key** [**0** | **7**] *key:* Defines the key for OSPF plain text authentication. **message-digest-key** *key-id* **md5** [**0** | **7**]key: Defines the key ID and key for OSPF MD5 authentication.

	authentication: Sets the authentication type to plain text authentication. **message-digest:** Sets the authentication type to MD5 authentication. **null:** Indicates that authentication is disabled.
Command Mode	OSPF routing process configuration mode
Usage Guide	In the OSPF routing domain, all areas must be connected to the backbone area. If the backbone area is disconnected, a virtual link must be configured to connect to the backbone area; otherwise, network communication problems will occur. A virtual link must be created between two ABRs, and the area to which both ABRs belong is the transit area. A stub area or an NSSA area cannot be used as a transit area. A virtual link can also be used to connect other non-backbone areas. **router-id** is the ID of an OSPF neighbor router. If you are sure about the value of **router-id**, run the **show ip ospf neighbor** command to confirm the value. You can configure the loopback address as the router ID. The **area virtual-link** command defines only the authentication key of the virtual link. To enable OSPF packet authentication in the areas connected to the virtual link, you must run the **area authentication** command. OSPF supports the Fast Hello function. After the OSPF Fast Hello function is enabled, OSPF finds neighbors and detects neighbor failures faster. You can enable the OSPF Fast Hello function by specifying the **minimal** and **hello-multiplier** keywords and the **multiplier** parameter. The **minimal** keyword indicates that the death interval is set to 1s, and **hello-multiplier** indicates the number of Hello packets sent per second. In this way, the interval at which the Hello packet is sent decreases to less than 1s. If the Fast Hello function is configured for a virtual link, the Hello interval field of the Hello packet advertised on the virtual link is set to 0, and the Hello interval field of the Hello packet received on this virtual link is ignored. No matter whether the Fast Hello function is enabled, the death interval must be consistent and the **hello-multiplier** values can be inconsistent on routers at both ends of the virtual link. Ensure that at least one Hello packet can be received within the death interval. Run the **show ip ospf virtual-links** command to monitor the death interval and Fast Hello interval configured for the virtual link. The **dead-interval minimal hello-multiplier** and **hello-interval** parameters introduced for the Fast Hello function cannot be configured simultaneously.

Configuration Example

Scenario	

	Remarks The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 B: GE 0/1 192.168.1.2 GE 0/2 192.168.3.1 C: GE 0/3 192.168.2.2 D: GE 0/3 192.168.3.2
Configuration Steps	● Configure the interface IP addresses on all routers. ● Enable the IPv4 unicast routing function on all routers. (This function is enabled by default.) ● Configure the OSPF instances and router IDs on all routers. ● Enable OSPF on the interfaces configured on all routers.
A	A#configure terminal A(config)#interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#ip address 192.168.1.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)#exit A(config)#interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)#ip address 192.168.2.1 255.255.255.0 A(config-if-GigabitEthernet 0/2)#exit A(config)#router ospf 1 A(config-router)#router-id192.168.1.1 A(config-router)#network 192.168.1.0 0.0.0.255 area 0 A(config-router)#network 192.168.2.0 0.0.0.255 area 1
B	B#configure terminal B(config)#interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)#ip address 192.168.1.2 255.255.255.0 B(config-if-GigabitEthernet 0/1)#exit B(config)#interface GigabitEthernet 0/2 B(config-if-GigabitEthernet 0/2)#ip address 192.168.3.1 255.255.255.0 B(config-if-GigabitEthernet 0/2)#exit B(config)#router ospf 1 B(config-router)#router-id192.168.1.2 B(config-router)#network 192.168.1.0 0.0.0.255 area 0 B(config-router)#network 192.168.3.0 0.0.0.255 area 2
C	C#configure terminal

	C(config)#interface GigabitEthernet 0/3 C(config-if-GigabitEthernet 0/3)#ip address 192.168.2.2 255.255.255.0 C(config-if-GigabitEthernet 0/3)#exit C(config)#router ospf 1 C(config-router)#router-id192.168.2.2 C(config-router)#network 192.168.2.0 0.0.0.255 area 1
D	D#configure terminal D(config)#interface GigabitEthernet 0/3 D(config-if-GigabitEthernet 0/3)#ip address 192.168.3.2 255.255.255.0 D(config-if-GigabitEthernet 0/3)#exit D(config)#router ospf 1 D(config-router)#router-id192.168.3.2 D(config-router)#network 192.168.3.0 0.0.0.255 area 2
Verification	● Verify that the OSPF neighbors are correct on all routers. ● Verify that the routing table is correctly loaded on all routers. ● On Router D, verify that the IP address 192.168.2.2 can be pinged successfully.
A	A# show ip ospf neighbor OSPF process 1, 2 Neighbors, 2 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.2 1 Full/DR 00:00:40192.168.1.2 GigabitEthernet 0/1 192.168.2.2 1 Full/BDR00:00:34 192.168.2.2 GigabitEthernet 0/2 A# show ip route ospf O IA 192.168.3.0/24 [110/2] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
B	B# show ip ospf neighbor OSPF process 1, 2 Neighbors, 2 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.1 1 Full/BDR 00:00:32 192.168.1.1 GigabitEthernet 0/1 192.168.3.2 1 Full/BDR00:00:30 192.168.3.2 GigabitEthernet 0/2 B# show ip route ospf

	O IA 192.168.2.0/24 [110/2] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
C	C# show ip ospf neighbor OSPF process 1,1 Neighbors,1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.1 1 Full/BDR 00:00:32 192.168.2.1 GigabitEthernet 0/3 C# show ip route ospf O IA 192.168.1.0/24 [110/2] via 192.168.2.1, 00:19:05, GigabitEthernet 0/3 O IA 192.168.3.0/24 [110/3] via 192.168.2.1, 00:19:05, GigabitEthernet 0/3
D	D# show ip ospf neighbor OSPF process 1,1 Neighbors,1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.21 Full/BDR00:00:30 192.168.3.1 GigabitEthernet 0/3 D# show ip route ospf O IA 192.168.1.0/24 [110/2] via 192.168.3.1, 00:19:05, GigabitEthernet 0/3 O IA 192.168.2.0/24 [110/3] via 192.168.3.1, 00:19:05, GigabitEthernet 0/3 D# ping 192.168.2.2 Sending 5, 100-byte ICMP Echoes to 192.168.2.2, timeout is 2 seconds: < press Ctrl+C to break > !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.

Common Errors

- OSPF cannot be enabled because the IP unicast routing function is disabled.
- The network segment configured by the **network** command does not include the interface IP addresses.
- The area IDs enabled on adjacent interfaces are inconsistent.
- The same router ID is configured on multiple routers, resulting in a router ID conflict.
- The same interface IP address is configured on multiple routers, resulting in a running error of the OSPF network.

5.4.2 Setting the Network Type

Configuration Effect

- Run OSPF to provide the IPv4 unicast routing serviceif the physical network is X.25, frame relay, or ATM.

Notes

- The OSPF basic functions must be configured.
- The broadcast network sends OSPF packets in multicast mode. Neighbors are automatically discovered, and the DR/BDR election is required.
- The P2P network sends OSPF packets in multicast mode. Neighbors are automatically discovered.
- The NBMA network sends OSPF packets in unicast mode. Neighbors must be manually specified, and the DR/BDR election is required.
- The P2MP network (without the **non-broadcast** parameter) sends OSPF packets in multicast mode. Neighbors are automatically discovered.
- The P2MP network (with the **non-broadcast** parameter) sends OSPF packets in unicast mode. Neighbors must be manually specified.

Configuration Steps

Configuring the Interface Network Type

- Optional.
- The configuration is required on routers at both ends of the link.

Configuring Neighbors

- (Optional) If the interface network type is set to NBMA or P2MP (with the **non-broadcast** parameter), neighbors must be configured.
- Neighbors are configured on routers at both ends of the NBMA or P2MP (with the **non-broadcast** parameter) network.

Configuring the Interface Priority

- (Optional) You must configure the interface priority if a router must be specified as a DR, or a router cannot be specified as a DR.
- Configure the interface priority on a router that must be specified as a DR, or cannot be specified as a DR.

Verification

- Run the **show ip ospf interface** command to verify that the network type of each interface is correct.

Related Commands

Configuring the Interface Network Type

Command	**ip ospf network** { **broadcast**| **non-broadcast**| **point-to-multipoint**[**non-broadcast**] | **point-to-point**}
Parameter Description	**broadcast**: Sets the interface network type to broadcast. **non-broadcast:** Sets the interface network type to non-broadcast. **point-to-multipoint** [**non-broadcast**]: Sets the interface network type to P2MP. If the interface does not have the broadcast capability, the **non-broadcast** parameter must be available. **point-to-point:** Sets the interface network type to P2P.
Command Mode	Interface configuration mode
Usage Guide	The broadcast type requires that the interface must have the broadcast capability.

	The P2P type requires that the interfaces are interconnected in one-to-one manner. The NBMA type requires full-meshed connections, and all interconnected routers can directly communicate with each other. The P2MP type does not raise any requirement.

Configuring Neighbors

Command	**neighbor** *ip-address* [**poll-interval***seconds*] [**priority***priority*] [**cost** *cost*]
Parameter Description	*ip-address*: Indicates the IP address of the neighbor interface. **poll-interval***seconds*: Indicates the neighbor polling interval. The unit is second. The value ranges from 0 to 2,147,483,647. This parameter is applicable only to the NBMA interface. **priority***priority*: Indicates the neighbor priority. The value ranges from 0 to 255. This parameter is applicable only to the NBMA interface. **cost***cost*: Indicates the cost required to reach each neighbor. There is no default value. The value ranges from 0 to 65,535. This parameter is applicable only to the P2MP interface.
Command Mode	OSPF routing process configuration mode
Usage Guide	Neighbors must be specified for the NBMA or P2MP (non-broadcast) interfaces. The neighbor IP address must be the primary IP address of this neighbor interface. If a neighbor router becomes inactive on the NBMA network, OSPF still sends Hello packets to this neighbor even if no Hello packet is received within the router death time. The interval at which the Hello packet is sent is called polling interval. When running for the first time, OSPF sends Hello packets only to neighbors whose priorities are not 0. In this way, neighbors with priorities set to 0 do not participate in the DR/BDR election. After a DR/BDR is elected, the DR/BDR sends the Hello packets to all neighbors to set up the adjacency. The P2MP (non-broadcast) network cannot dynamically discover neighbors because it does not have the broadcast capability. Therefore, you must use this command to manually configure neighbors for the P2MP (non-broadcast) network. In addition, you can use the **cost** parameter to specify the cost to reach each neighbor on the P2MP network.

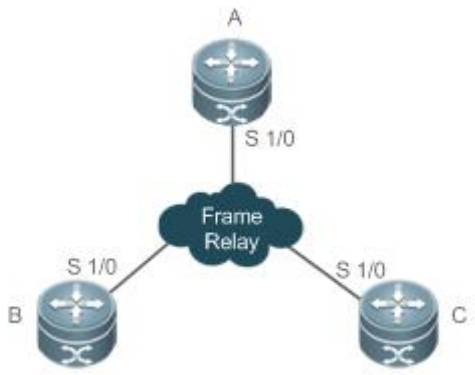
Configuring the Interface Priority

Command	**ip ospf priority** *priority*
Parameter Description	*priority*: Indicates the OSPF priority of an interface. The value ranges from 0 to 255.
Command Mode	Interface configuration mode
Usage Guide	The OSPF interface priority is contained in the Hello packet. When the DR/BDR election occurs on the OSPF broadcast network, the router with the highest priority becomes the DR or BDR. If the priorities are the same, the router with the largest router ID becomes the DR or BDR. A router with the priority set to 0 does not participate in the DR/BDR election. This command is applicable only to the OSPF broadcast and NBMA interfaces.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 5.4.1 "Configuring OSPF Basic Functions."

Setting the Interface Network Type to P2MP

Scenario	 **Remarks** The interface IP addresses are as follows: A: S1/0 192.168.1.2 B: S1/0 192.168.1.3 C: S1/0 192.168.1.4
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Set the interface network type to P2MP on all routers.
A	A#configure terminal A(config)# interface Serial1/0 A(config-Serial1/0)# encapsulation frame-relay A(config-Serial1/0)# ip ospf network point-to-multipoint
B	B#configure terminal B(config)# interface Serial1/0 B(config-Serial1/0)# encapsulation frame-relay B(config-Serial1/0)# ip ospf network point-to-multipoint
C	C#configure terminal C(config)# interface Serial1/0 C(config-Serial1/0)# encapsulation frame-relay C(config-Serial1/0)# ip ospf network point-to-multipoint

Verification	Verify that the interface network type is P2MP. A# show ip ospf interface Serial1/0 Serial1/0 is up, line protocol is up Internet Address 192.168.1.2/24, Ifindex 2, Area 0.0.0.1, MTU 1500 Matching network config: 192.168.1.0/24 Process ID 1, Router ID 192.168.1.2, Network Type POINTOMULTIPOINT, Cost: 1 Transmit Delay is 1 sec, State Point-To-Point Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in 00:00:02 Neighbor Count is 1, Adjacent neighbor count is 0 Crypt Sequence Number is 4787 Hello received 465 sent 466, DD received 8 sent 8 LS-Req received 2 sent 2, LS-Upd received 8 sent 21 LS-Ack received 14 sent 7, Discarded 3

Common Errors

- The network types configured on interfaces at two ends are inconsistent, causing abnormal route learning.
- The network type is set to NBMA or P2MP (with the **non-broadcast** parameter), but neighbors are not specified.

5.4.3 Configuring Route Redistribution and Default Route

Configuration Effect

- In the OSPF domain, introduce a unicast route to other AS domains so that the unicast routing service to other AS domainscan be provided for users in the OSPF domain.
- In the OSPF domain, inject a default route to other AS domains so that the unicast routing service to other AS domains can be provided for users in the OSPF domain.

Notes

- The OSPF basic functions must be configured.

Configuration Steps

Configuring External Route Redistribution

- (Optional) This configuration is required if external routes of the OSPF domain should be introduced to an ASBR.
- This configuration is performed on an ASBR.

Generating a Default Route

- (Optional) This configuration is required if the default route should be introduced to an ASBR so that other routers in the OSPF domain access other AS domains through this ASBR by default.

- This configuration is performed on an ASBR.

Verification

- On a router inside the OSPF domain, run the **show ip route** command to verify that the unicast routes to other AS domains are loaded.
- On a router inside the OSPF domain, run the **show ip route** command to verify that the default route to the ASBR is loaded.
- Run the **ping** command to verify that the IPv4 unicast service to other AS domains is correct.

Related Commands

Configuring External Route Redistribution

Command	**redistribute** { **connected** | **ospf***process-id* | **rip** | **static** }[**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] [**metric** *metric-value*] [**metric-type** { **1** | **2** }] [**route-map** *route-map-name*] [**subnets**] [**tag***tag-value*]
Parameter Description	**connected:** Indicates redistribution from direct routes. **ospf** *process-id:* Indicates redistribution from OSPF.*process-id* specifies an OSPF process. The value ranges from 1 to 65,535. **rip:** Indicates redistribution from RIP. **static:** Indicates redistribution from static routes. **match:** Used only when OSPF routes are redistributed. Only the routes meeting the filtering conditions are redistributed. By default, all OSPF routes can be redistributed. **metric** *metric-value:* Specifies the metric of the OSPF external LSA. *metric-value* specifies the size of the metric. The value ranges from 0 to 16,777,214. **metric-type** { **1** | **2** }: Setsthe external route type, which can be E-1 or E-2. **route-map** *route-map-name:* Setsthe redistribution filtering rules. **subnets:** Specifiesthe non-standard networks for redistribution. **tag** *tag-value:* Specifies the tag value of the route that is redistributed into the OSPF routing domain. The value ranges from 0 to 4,294,967,295.
Command Mode	OSPF routing process configuration mode
Usage Guide	After this command is configured, the router becomes an ASBR, imports related routing information to the OSPF domain, and advertises the routing information as Type 5 LSAs to other OSPF routers in the domain. If you configure redistribution of OSPF routes without specifying the **match** parameter, OSPF routes of all sub-types can be distributed by default. The latest setting of the **match** parameter is used as the initial **match** parameter. Only routes that match the sub-types can be redistributed. You can use the **no** form of the command to restore the default value of **match**. For details, see the configuration example. If **route-map** is specified, the filtering rules specified in **route-map** are applicable to original parameters of redistribution. For redistribution of OSPF route, the routemap is used for filtering only when the redistributed routes meet criteria specified by **match**. The **set metric** value associated with **route-map** should fall into the range of 0 to 16,777,214. If the value exceeds this range, routes cannot be introduced. The configuration rules for the **no** form of the **redistribute** command are as follows: 1. If some parameters are specified in the **no** form of the command, default values of these parameters will be restored. 2. If no parameter is specified in the **no** form of the command, the entire command will be deleted.

Introducing a Default Route

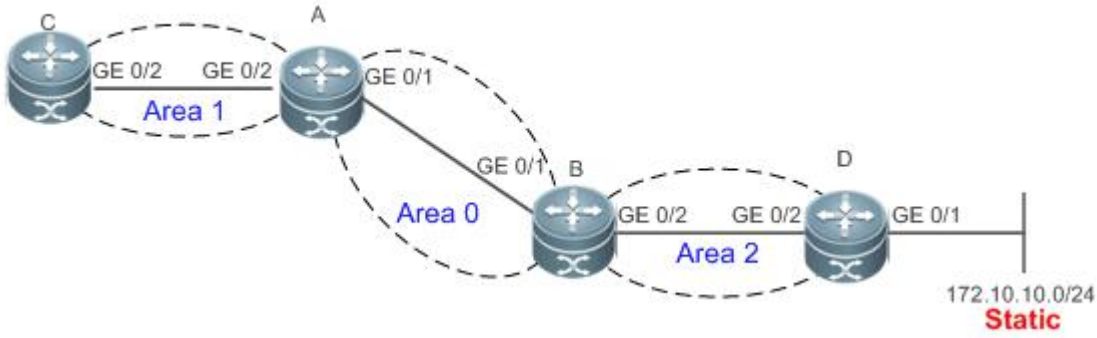
Command	**default-information originate** [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map***map-name*]
Parameter Description	**always:** Enables OSPF to generate a default route regardless of whether the local router has a default route. **metric** *metric:* Indicates the initial metric of the default route. The value ranges from 0 to 16,777,214. **metric-type***type:* Indicates the type of the default route. OSPF external routes are classified into two types: Type 1: The metric varies with routers; Type 2: The metric is the same for all routers. Type 1 external routes are more trustworthy than Type 2 external routes. **route-map** *map-name:* Indicates the associated route-map name. By default, no route-map is associated.
Command Mode	OSPF routing process configuration mode
Usage Guide	When the **redistribute** or **default-information** command is executed, the OSPF router automatically becomes an ASBR. The ASBR, however, does not automatically generate or advertise a default route to all routers in the OSPF routing domain. To have the ASBR generates a default route, configure the **default-information originate** command. If **always** is specified, the OSPF routing process advertises an external default route to neighbors regardless of whether a default route exists. This default route, however, is not displayed on the local router. To confirm whether the default route is generated, run the **show ip ospf database** command to display the OSPF link status database. The external link with the ID 0.0.0.0 describes the default route. On an OSPF neighbor, you can run the **show ip route** command to see the default route. The metric of the external default route can only be defined in the **default-information originate** command, instead of the **default-metric** command. OSPF has two types of external routes. The metric of the Type 1 external route changes, but the metric of the Type 2 external route is fixed. If two parallel paths to the same destination have the same route metric, the priority of the Type 1 route is higher than that of the Type 2 route. Therefore, the **show ip route** command displays only the Type 1 route. A router in the stub area cannot generate an external default route. The **set metric** value associated with **route-map** should fall into the range of 0 to 16,777,214. If the value exceeds this range, routes cannot be introduced.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 5.4.1 "Configuring OSPF Basic Functions."

Configuring Static Route Redistribution

Scenario



Remarks	The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 B: GE 0/1 192.168.1.2 GE 0/2 192.168.3.1 C: GE 0/2 192.168.2.2 D: GE 0/1 192.168.6.2 GE 0/2 192.168.3.2

Configuration Steps

- Configure the interface IP addresses on all routers. (Omitted)
- Configure the OSPF basic functions on all routers. (Omitted)
- Introduce an external static route to Router D.

D

```
D# configure terminal
D(config)# ip route 172.10.10.0 255.255.255.255.0 192.168.6.3
D(config)#router ospf 1
D(config-router)# redistribute staticsubnets
```

Verification

- On Router D, run the **show ip ospf database external brief** command to verify that an LSA corresponding to an external route is generated.
- On Router C, run the **show ip route ospf** command to verify that the external static route has been introduced.

D

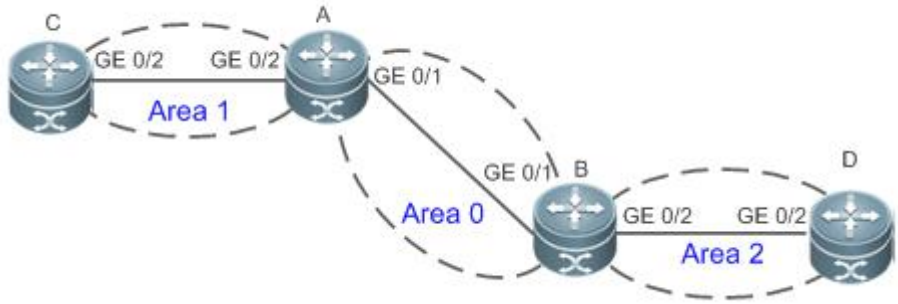
```
D# show ip ospf database external brief
                OSPF Router with ID (192.168.22.30) (Process ID 1)
                    AS External Link States

Link ID         ADV Router      Age  Seq#       CkSum  Route                Tag
172.10.10.0     192.168.22.30   11   0x80000001 0xa4bb E2 172.10.10.0/24     0
```

C

```
C# show ip route ospf
O E2 172.10.10.0/24 [110/20] via 192.168.2.1, 00:18:03, GigabitEthernet 0/2
```

Configuring the Default Route

Scenario



Remarks	The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 B: GE 0/1 192.168.1.2 GE 0/2 192.168.3.1 C: GE 0/2 192.168.2.2 D: GE 0/2 192.168.3.2

Configuration Steps

- Configure the interface IP addresses on all routers. (Omitted)
- Configure the OSPF basic functions on all routers. (Omitted)
- Configure the default route on Router D.

D

```
D# configure terminal
D(config)#router ospf 1
D(config-router)#default-information originate always
```

Verification

- On Router D, run the **show ip ospf database external brief** command to verify that an LSA corresponding to the default route is generated.
- On Router C, run the **show ip route ospf** command to verify that the OSPF default route exists.

D

```
D#show ip ospf database external brief
                OSPF Router with ID (192.168.22.30) (Process ID 1)
                    AS External Link States

Link ID         ADV Router      Age  Seq#       CkSum  Route          Tag
0.0.0.0         192.168.22.30   565  0x80000002 0xa190 E2 0.0.0.0/0    1
```

C

```
C# show ip route ospf
O E20.0.0.0/0 [110/20] via 192.168.2.1, 00:18:03, GigabitEthernet 0/2
```

Common Errors

- The subnet route is not introduced because the **subnets** parameter in the **redistribute** command is not configured.
- A routing loop is formed because the **default-information originate always** command is configured on multiple routers.
- Routes cannot be introduced because route redistribution is configured on a router in the stub area.

5.4.4 Configuring Stub Area and NSSA Area

Configuration Effect

- Configure an area located on the stub as a stub area to reduce interaction of routing information and the size of routing table, and enhance stability of routes.

Notes

- The OSPF basic functions must be configured.
- A backbone or transit area cannot be configured as a stub or an NSSA area.
- A router in the stub area cannot introduce external routes, but a router in the NSSA area can introduce external routes.

Configuration Steps

Configuring a Stub Area

- (Optional) This configuration is required if you wish to reduce the size of the routing table on routers in the area.
- The area must be configured as a stub area on all routers in this area.

Configuring an NSSA Area

- (Optional) This configuration is required if you wish to reduce the size of the routing table on routers in the area and introduce OSPF external routes to the area.
- The area must be configured as an NSSA area on all routers in this area.

Verification

Verifying the Stub Area

- On a router in the stub area, run the **show ip route** command to verify that the router is not loaded with any external routes.

Verifying the NSSA Area

- On a router in the NSSA area, run the **show ip ospf database** command to verify that the introduced external route generates Type 7 LSAs.
- On a router in the backbone area, run the **show ip route** command to verify that the router is loaded with external routes introduced from the NSSA area.

Related Commands

Configuring a Stub Area

Command	**area** *area-id* **stub** [**no-summary**]

Parameter Description	*area-id:* Indicates the ID of the stub area. **no-summary:** Prohibits the ABR from sending network summary LSAs. At this time, the stub can be called totally stub area. This parameter is configured only when the router is an ABR.
Command Mode	OSPF routing process configuration mode
Usage Guide	You must run the **area stub** command on all routers in the OSPF stub area. The ABR sends only three types of LSAs to the stub area: (1) Type 1: Router LSA; (2) Type 2: Network LSA; (3) Type 3: Network Summary LSA. From the routing table point of view, a router in the stub area can learn only the internal routes of the OSPF routing domain, including the internal default route generated by an ABR. A router in the stub area cannot learn external routes of the OSPF routing domain. To configure a totally stub area, add the **no-summary** keyword when running the **area stub** command on the ABR. A router in the totally stub area can learn only the internal routes of the local area, including the internal default route generated by an ABR. You can run either the **area stub** or **area default-cost** command to configure an OSPF area as a stub area. If **area stub** is used, you must configure this command on all routers connected to the stub area. If **area default-cost** is used, run this command only on the ABR in the stub area. The **area default-cost** command defines the initial cost (metric) of the internal default route.

Configuring an NSSA Area

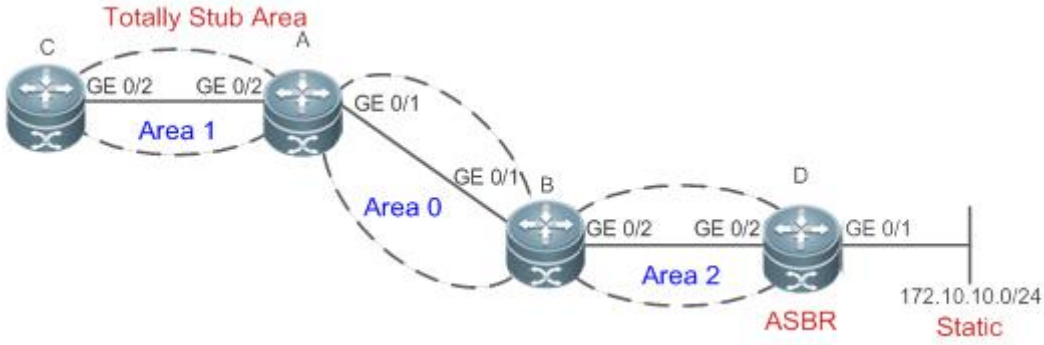
Command	**area** *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric** *value*] [**metric-type** *type*]] [**no-summary**] [**translator** [**stability-interval** *seconds* | **always**]]
Parameter Description	*area-id:* Indicates the ID of the NSSA area. **no-redistribution:** Select this option if the router is an NSSA ABR and you want to use only the **redistribute** command to introduce the routing information into a common area instead of an NSSA area. **default-information-originate:** Indicates that a default Type 7 LSA is generated and introduced to the NSSA area. This option takes effect only on an NSSA ABR or ASBR. **metric***value:* Specifies the metric of the generated default LSA. The value ranges from 0 to 16,777,214. The default value is 1. **metric-type***type:* Specifies the route type of the generated default LSA. The values include 1 and 2. **1** represents N-1, and **2** represents N-2. The default value is 2. **no-summary:** Prohibits the ABR in the NSSA area from sending summary LSAs (Type-3 LSA). **translator:** Indicatesthat the NSSA ABR is a translator. **stability-interval***seconds:* Indicates the stability interval after the NSSA ABR is changed from a translator to a non-translator. The unit is second. The default value is 40. The value ranges from 0 to 2,147,483,647. **always:** Indicates that the current NSSA ABR always acts as a translator. The default value is the standby translator.
Command Mode	OSPF routing process configuration mode
Usage Guide	The **default-information-originate** parameter is used to generate a default Type 7 LSA. This parameter has different functions on the ABR and the ASBR in the NSSA area. On the ABR, a Type 7 LSA default route is generated regardless of whether the default route exists in the routing table. On the ASBR (not an ABR), a Type 7 LSA default route is generated only when the default route exists in the routing table. If the **no-redistribution** parameter is configured on the ASBR, other external routes introduced by OSPF through the **redistribute** command cannot be advertised to the NSSA area. This parameter is generally used when a router in the NSSA area acts both as the ASBR and the ABR. It prevents external routing information from entering the NSSA area.

	To further reduce the number of LSAs sent to the NSSA area, you can configure the **no-summary** parameter on the ABR to prevent the ABR from sending the summary LSAs (Type 3 LSA) to the NSSA area. **area default-cost** is used on an ABR or ASBR connected to the NSSA area. This command configures the cost of the default route sent from the ABR/ASBR to the NSSA area. By default, the cost of the default route sent to the NSSA area is 1. If an NSSA area has two or more ABRs, the ABR with the largest router ID is elected by default as the translator for converting Type 7 LSAs into Type 5 LSAs. If the current device is always the translator ABR for converting Type 7 LSAs into Type 5 LSAs, use the **translator always** parameter. If the translator role of the current device is replaced by another ABR, the conversion capability is retained during the time specified by **stability-interval**. If the router does not become a translator again during **stability-interval**, LSAs that are converted from Type 7 to Type 5 will be deleted from the AS after **stability-interval** expires. To prevent a routing loop, LSAs that are converted from Type 7 to Type 5 will be deleted from the AS immediately after the current device loses the translator role even if **stability-interval** does not expire. In the same NSSA area, it is recommended that **translator always** be configured on only one ABR.

Configuration Example

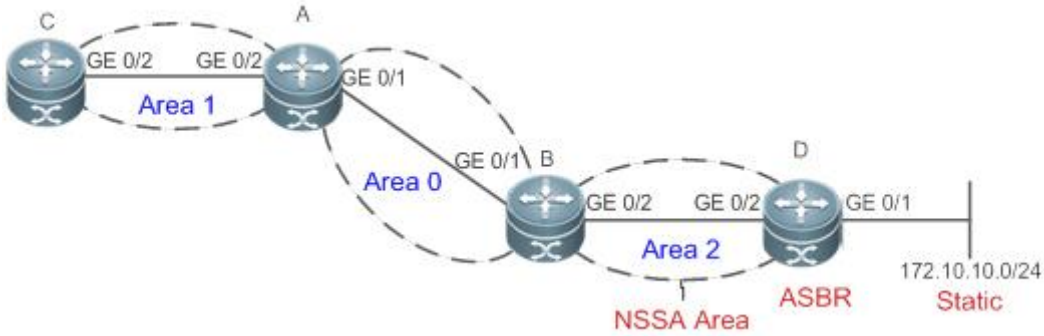
The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 5.4.1 "Configuring OSPF Basic Functions."

Configuring a Stub Area

Scenario	 **Remarks**: The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 B: GE 0/1 192.168.1.2 GE 0/2 192.168.3.1 C: GE 0/2 192.168.2.2 D: GE 0/1 192.168.6.2 GE 0/2 192.168.3.2
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Introduce an external static route to Router D. ● Configure area 1 as the stub area on Router A and Router C.

D	D# configure terminal D(config)#router ospf 1 D(config-router)# redistribute staticsubnets
A	A# configure terminal A(config)#router ospf 1 A(config-router)#area 1 stubno-summary
C	C# configure terminal C(config)#router ospf 1 C(config-router)#area 1 stub
Verification	On Router C, run the **show ip route ospf** command to display the routing table. Verify that there is only one default inter-area route, and no external static route is introduced from Router D.
	C#show ip route ospf O*IA 0.0.0.0/0 [110/2] via 192.168.2.1, 00:30:53, GigabitEthernet 0/2

Configuring an NSSA Area

Scenario	 **Remarks**: The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 B: GE 0/1 192.168.1.2 GE 0/2 192.168.3.1 C: GE 0/2 192.168.2.2 D: GE 0/1 192.168.6.2 GE 0/2 192.168.3.2
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Introduce an external static route to Router D. ● Configure area 2 as the NSSA area on Router B and Router D.

B	B# configure terminal B(config)#router ospf 1 B(config-router)#area 2 nssa
D	D# configure terminal D(config)#ip route 172.10.10.0 255.255.255.0 192.168.6.2 D(config)#router ospf 1 D(config-router)#redistribute static subnets D(config-router)#area 2 nssa
Verification	● On Router D, verify that the Type 7 LSA, 172.10.10.0/24, is generated. ● On Router B, verify that Type 5 and Type 7 LSAs coexist on 172.10.10.0/24. ● On Router B, verify that the N-2 route of 172.10.10.0/24 is generated.
D	D# show ip ospf database nssa-external OSPF Router with ID (192.168.6.2) (Process ID 1) NSSA-external Link States (Area 0.0.0.1 [NSSA]) LS age: 61 Options: 0x8 (-|-|-|-|N/P|-|-|-) LS Type: AS-NSSA-LSA Link State ID: 172.10.10.0 (External Network Number For NSSA) Advertising Router: 192.168.6.2 LS Seq Number: 80000001 Checksum: 0xc8f8 Length: 36 Network Mask: /24 Metric Type: 2 (Larger than any link state path) TOS: 0 Metric: 20 NSSA: Forward Address: 192.168.6.2 External Route Tag: 0
B	B# show ip ospf database nssa-external OSPF Router with ID (192.168.3.1) (Process ID 1) NSSA-external Link States (Area 0.0.0.1 [NSSA])

```
  LS age: 314
  Options: 0x8 (-|-|-|-|N/P|-|-|-)
  LS Type: AS-NSSA-LSA
  Link State ID: 172.10.10.0 (External Network Number For NSSA)
  Advertising Router: 192.168.6.2
  LS Seq Number: 80000001
  Checksum: 0xc8f8
  Length: 36
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        NSSA: Forward Address: 192.168.6.2
        External Route Tag: 0
B# show ip ospf database external
            OSPF Router with ID (192.168.3.1) (Process ID 1)
                AS External Link States
  LS age: 875
  Options: 0x2 (-|-|-|-|-|-|E|-)
  LS Type: AS-external-LSA
  Link State ID: 172.10.10.0 (External Network Number)
  Advertising Router: 192.168.3.1
  LS Seq Number: 80000001
  Checksum: 0xd0d3
  Length: 36
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        Forward Address: 192.168.6.2
        External Route Tag: 0

B# show ip route ospf
O N2    172.10.10.0/24 [110/20] via 192.168.3.2, 00:06:53, GigabitEthernet 0/2
```

Common Errors

- Configurations of the area type are inconsistent on routers in the same area.
- External routes cannot be introduced because route redistribution is configured on a router in the stub area.

5.4.5 Configuring Route Summarization

Configuration Effect

- Summarize routes to reduce interaction of routing information and the size of routing table, and enhance stability of routes.
- Shield or filter routes.

Notes

- The OSPF basic functions must be configured.
- The address range of summarized routes may exceed the actual network range in the routing table. If data is sent to a network beyond the summarization range, a routing loop may be formed and the router processing load may increase. To prevent these problems, a discard route must be added to the routing table or shield or filter routes.

Configuration Steps

Configuring Inter-Area Route Summarization

- (Optional) This configuration is required when routes of the OSPF area need to be summarized.
- Unless otherwise required, this configuration should be performed on an ABR in the area where routes to be summarized are located.

Configuring External Route Summarization

- (Optional) This configuration is required when routes external to the OSPF domain need to be summarized.
- Unless otherwise required, this configuration should be performed on an ASBR to which routes to be summarized are introduced.

Verification

Run the **show ip route ospf** command to verify that individual routes do not exist and only the summarized route exists.

Related Commands

Configuring Inter-Area Route Summarization

Command	**area** *area-id* **range** *ip-address net-mask* [**advertise** | **not-advertise**] [**cost** *cost*]
Parameter Description	*area-id*: Specifies the ID of the OSPF area to which the summarized route should be injected. The area ID can be a decimal integer or an IP address. *ip-address net-mask*: Defines the network segment of the summarized route. **advertise** | **not-advertise**: Specifies whether the summarized route should be advertised. **cost** *cost:* Indicates the metric of the summarized route. The value ranges from 0 to 16777215.
Command Mode	OSPF routing process configuration mode
Usage Guide	This command can be executed only on the ABR. It is used to combine or summarize multiple routes of an area into one

	route, and advertise the route to other areas. Combination of the routing information occurs only on the boundary of an area. Routers inside the area can learn specific routing information, whereas routers in other areas can learn only one summarized route. In addition, you can set **advertise** or **not-advertise** to determine whether to advertise the summarized route to shield and filter routes. By default, the summarized route is advertised. You can use the **cost** parameter to set the metric of the summarized route. You can configure route summarization commands for multiple areas. This simplifies routes in the entire OSPF routing domain, and improve the network forwarding performance, especially for a large-sized network. When multiple route summarization commands are configured and have the inclusive relationship with each other, the area range to be summarized is determined based on the maximum match principle.

Configuring External Route Summarization

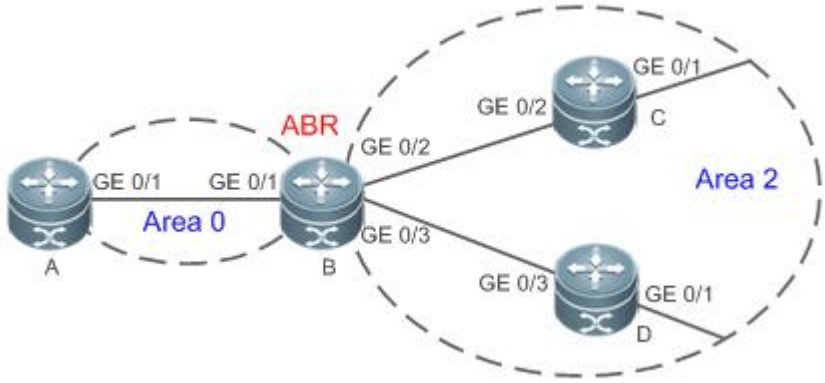
Command	**summary-address** *ip-address net-mask* [**not-advertise** | **tag** *value*]
Parameter Description	*ip-address*: Indicates the IP address of the summarized route. *net-mask*: Indicates the subnet mask of the summarized route. **not-advertise**: Indicates that the summarized route is not advertised. If this parameter is not specified, the summarized route is advertised. **tag***value:* Indicates the tag of the summarized route. The value ranges from 0 to 4,294,967,295.
Command Mode	OSPF routing process configuration mode
Usage Guide	When routes are redistributed from other routing processes and injected to the OSPF routing process, each route is advertised to the OSPF routers using an external LSA. If the injected routes are a continuous address space, the ABR can advertised only one summarized route to significantly reduce the size of the routing table. **area range** summarizesthe routes between OSPF routes, whereas **summary-address** summarizes external routes of the OSPF routing domain. When configured on the NSSA ABR translator, **summary-address** summarizes redistributed routes and routes obtained based on the LSAs that are converted from Type 7 to Type 5. When configured on the ASBR (not an NSSA ABR translator), **summary-address** summarizes only redistributed routes.

Configuring a Discard Route

Command	**discard-route** { **internal** | **external** }
Parameter Description	**internal:** Indicates that the discard route generated by the **area range** command can be added. **external:** Indicates that the discard route generated by the **summary-address** command can be added.
Command Mode	OSPF routing process configuration mode
Usage Guide	The address range of summarized routes may exceed the actual network range in the routing table. If data is sent to a network beyond the summarization range, a routing loop may be formed and the router processing load may increase. To prevent these problems, a discard route must be added to the routing table on the ABR or ASBR. This route is automatically generated, and is not advertised.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 5.4.1 "Configuring OSPF Basic Functions."

Scenario	 **Remarks**: The interface IP addresses are as follows: A: GE0/1 192.168.1.1 B: GE0/1 192.168.1.2 GE0/2 172.16.2.1 GE0/3 172.16.3.1 C: GE0/2 172.16.2.2 GE0/1 172.16.4.2 D: GE0/2 172.16.3.2 GE0/1 172.16.5.2
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Summarize routes of area 2 on Router B.
B	B# configure terminal B(config)#router ospf 1 B(config-router)#area 2 range 172.16.0.0 255.255.0.0
Verification	On Router A, verify that the entry 172.16.0.0/16 is added to the routing table.
A	A#show ip route ospf O IA 172.16.0.0/16 [110/2] via 192.168.1.2, 00:01:04, GigabitEthernet 0/1

Common Errors

- Inter-area route summarization cannot be implemented because the **area range** command is configured on a non-ABR device.

5.4.6 Configuring Route Filtering

Configuration Effect

- Routes that do not meet filtering conditions cannot be loaded to the routing table, or advertised to neighbors. Network users cannot access specified destination network.

Notes

- The OSPF basic functions must be configured.
- Filtering routes by using the **distribute-list in** command affects forwarding of local routes, but does not affect route computation based on LSAs. Therefore, if route filtering is configured on the ABR, Type 3 LSAs will still be generated and advertised to other

areas because routes can still be computed based on LSAs. As a result, black-hole routes are generated. In this case, you can run the **area filter-list** or **area range** (containing the **not-advertise** parameter) command on the ABR to prevent generation of black-hole routes.

Configuration Steps

Configuring Inter-Area Route Filtering

- (Optional) This configuration is recommended if users should be restricted from accessing the network in a certain OSPF area.
- Unless otherwise required, this configuration should be performed on an ABR in the area where filtered routes are located.

Configuring Redistributed Route Filtering

- (Optional) This configuration is required if external routes introduced by the ASBR need to be filtered.
- Unless otherwise required, this configuration should be performed on an ASBR to which filtered routes are introduced.

Configuring Learned Route Filtering

- (Optional) This configuration is required if users should be restricted from accessing a specified destination network.
- Unless otherwise required, this configuration should be performed on a router that requires route filtering.

Verification

- Run the **show ip route** command to verify that the router is not loaded with routes that have been filtered out.
- Run the **ping** command to verify that the specified destination network cannot be accessed.

Related Commands

Configuring a Passive Interface

Command	**passive-interface**{ **default** | *interface-type interface-number* | *interface-type interface-numberip-address*}
Parameter Description	*interface-type interface-number*: Indicates the interface that should be configured as a passive interface. **default:** Indicates that all interface will be configured as passive interfaces. *interface-type interface-numberip-address:* Specifies an address of the interface as the passive address.
Command Mode	OSPF routing process configuration mode
Usage Guide	To prevent other routers on the network from learning the routing information of the local router, you can configure a specified network interface of the local router as the passive interface, or a specified IP address of a network interface as the passive address.

Configuring the LSA Update Packet Filtering

Command	**ip ospf database-filter all out**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Enable this function on an interface to prevent sending the LSA update packet on this interface. After this function is enabled, the local router does not advertise the LSA update packet to neighbors, but still sets up the adjacency with

	neighbors and receives LSAs from neighbors.

Configuring Inter-Area Route Filtering

Command	**area***area-id***filter-list** {**access***acl-name*| **prefix** *prefix-name*} {**in** | **out**}
Parameter Description	*area-id*: Indicates the area ID. **access** *acl-name*: Indicates the associated ACL. **prefix** *prefix-name*: Indicates the associated prefix list. **in** | **out:** Filters routes that are received by or sent from the area.
Command Mode	OSPF routing process configuration mode
Usage Guide	This command can be configured only on an ABR. Use this command when it is required to configure filtering conditions for inter-area routes on the ABR.

Configuring Redistributed Route Filtering

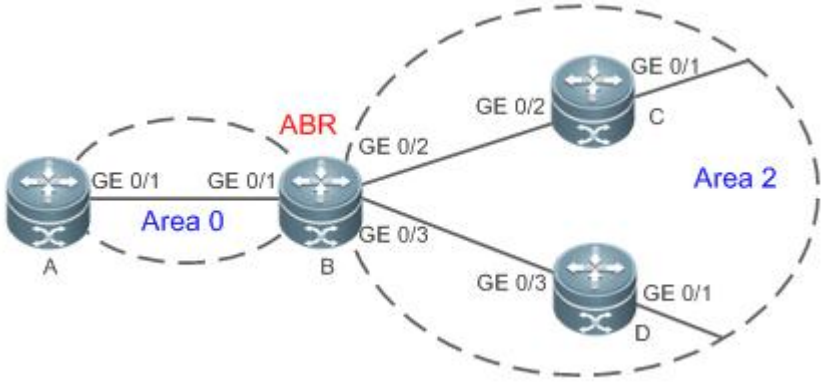
Command	**distribute-list** { [*access-list-number* | *name*] | **prefix** *prefix-list-name* } **out** [**connected** | **ospf** *process-id* | **rip** | **static**]
Parameter Description	*access-list-number* | *name*: Uses the ACL for filtering. **prefix** *prefix-list-name*: Uses the prefixlist for filtering. **connected** | **ospf** *process-id* | **rip** | **static**: Indicates the source of routes to be filtered.
Command Mode	OSPF routing process configuration mode
Usage Guide	**distribute-list out** is similar to **redistribute route-map**, and is used to filter routes that are redistributed from other protocols to OSPF. The **distribute-list out** command itself does not redistribute routes, and is generally used together with the **redistribute** command. The ACL and the prefixlist filtering rules are mutually exclusive in the configuration. That is, if the ACL is used for filtering routes coming from a certain source, the prefixlist cannot be configured to filter the same routes.

Configuring Learned Route Filtering

Command	**distribute-list** {[*access-list-number* | *name*] | **prefix***prefix-list-name* [**gateway** *prefix-list-name*] | **route-map** *route-map-name* } **in** [*interface-typeinterface-number*]
Parameter Description	*access-list-number* | *name*: Uses the ACL for filtering. **gateway***prefix-list-name*: Uses the gateway for filtering. **prefix***prefix-list-name*: Uses the prefixlist for filtering. **route-map** *route-map-name:* Uses the route map for filtering. *interface-type interface-number:* Specifies the interface for which LSA routes are filtered.
Command Mode	OSPF routing process configuration mode
Usage Guide	Filter routes that are computed based on received LSAs. Only routes meeting the filtering conditions can be forwarded. The command does not affect the LSDB or the routing tables of neighbors. The ACL, prefix list, and route map filtering rules are mutually exclusive in the configuration. That is, if the ACL is used for filtering routes of a specified interface, the prefix list or router map cannot be configured for filtering routes of the same interface.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 5.4.1 "Configuring OSPF Basic Functions."

Scenario	 **Remarks**: The interface IP addresses are as follows: A: GE0/1 192.168.1.1 B: GE0/1 192.168.1.2 GE0/2 172.16.2.1 GE0/3 172.16.3.1 C: GE0/2 172.16.2.2 GE0/3 172.16.4.2 D: GE0/2 172.16.3.2 GE0/3 172.16.5.2
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router A, configure route filtering.
A	A# configure terminal A(config)#access-list 3 permit host 172.16.5.0 A(config)#router ospf 1 A(config-router)#distribute-list 3 in GigabitEthernet 0/1
Verification	● On Router A, check the routing table. Verify that only the entry 172.16.5.0/24 is loaded.
A	A# show ip route ospf O 172.16.5.0/24 [110/2] via 192.168.1.2, 10:39:40, GigabitEthernet 0/1

Common Errors

- Filtering routes by using the **distribute-list in** command affects forwarding of local routes, but does not affect route computation based on LSAs. Therefore, if route filtering is configured on the ABR, Type 3 LSAs will still be generated and advertised to other areas because routes can still be computed based on LSAs. As a result, black-hole routes are generated.

5.4.7 Modifying Route Cost and AD

Configuration Effect

- Change the OSPF routes to enable the traffic pass through specified nodes or avoid passing through specified nodes.
- Change the sequence that a router selects routes so as to change the priorities of OSPF routes.

Notes

- The OSPF basic functions must be configured.
- If you run the **ip ospf cost** command to configure the cost of an interface, the configured cost will automatically overwrite the cost that is computed based on the auto cost.

Configuration Steps

Configuring the Reference Bandwidth

- Optional.
- A router is connected with lines with different bandwidths. This configuration is recommended if you wish to preferentially select the line with a larger bandwidth.

Configuring the Cost of an Interface

- Optional.
- A router is connected with multiple lines. This configuration is recommended if you wish to manually specify a preferential line.

Configuring the Default Metric for Redistribution

- Optional.
- This configuration is mandatory if the cost of external routes of the OSPF domain should be specified when external routes are introduced to an ASBR.

Configuring the Maximum Metric

- Optional.
- A router may be unstable during the restart process or a period of time after the router is restarted, and users do not want to forward data through this router. In this case, this configuration is recommended.

Configuring the AD

- Optional.
- This configuration is mandatory if you wish to change the priorities of OSPF routes on a router that runs multiple unicast routing protocols.

Verification

- Run the **show ip ospf interface** command to verify that the costs of interfaces are correct.
- Run the **show ip route** command to verify that the costs of external routes introduced to the ASBR are correct.
- Restart the router. Within a specified period of time, data is not forwarded through the restarted router.

Related Commands

Configuring the Reference Bandwidth

Command	**auto-cost reference-bandwidth** *ref-bw*
Parameter Description	*ref-bw*: Indicates the reference bandwidth. The unit is Mbps. The value ranges from 1 to 4,294,967.
Command	OSPF routing process configuration mode

Mode	
Usage Guide	By default, the cost of an OSPF interface is equal to the reference value of the auto cost divided by the interface bandwidth. Run the **auto-cost** command to obtain the reference value of the auto cost. The default value is 100 Mbps. Run the **bandwidth** command to set the interface bandwidth. The costs of OSPF interfaces on several typical lines are as follows: 64Kbps serial line: The cost is 1562. E1 line: The cost is 48. 10M Ethernet: The cost is 10. 100M Ethernet: The cost is 1. If you run the **ip ospf cost** command to configure the cost of an interface, the configured cost will automatically overwrite the cost that is computed based on the auto cost.

Configuring the Cost of an Interface

Command	**ip ospf cost***cost*
Parameter Description	*cost*: Indicates the cost of an OSPF interface. The value ranges from 0 to 65,535.
Command Mode	Interface configuration mode
Usage Guide	By default, the cost of an OSPF interface is equal to the reference value of the auto cost divided by the interface bandwidth. Run the **auto-cost** command to obtain the reference value of the auto cost. The default value is 100 Mbps. Run the **bandwidth** command to set the interface bandwidth. The costs of OSPF interfaces on several typical lines are as follows: 64Kbps serial line: The cost is 1562. E1 line: The cost is 48. 10M Ethernet: The cost is 10. 100M Ethernet: The cost is 1. If you run the **ip ospf cost** command to configure the cost of an interface, the configured cost will automatically overwrite the cost that is computed based on the auto cost.

Configuring the Cost of the Default Route in a Stub or an NSSA Area

Command	**area***area-id* **default-cost***cost*
Parameter Description	*area-id*: Indicates the ID of the stub or NSSA area. *cost*: Indicates the cost of the default summarized route injected to the stub or NSSA area. The value ranges from 0 to 16,777,215.
Command Mode	OSPF routing process configuration mode
Usage Guide	This command takes effect only on an ABR in a stub area or an ABR/ASBR in an NSSA area. An ABR in a stub area or an ABR/ASBR in an NSSA area is allowed to advertise an LSA indicating the default route in the stub or NSSA area. You can run the **area default-cost** command to modify the cost of the advertised LSA.

Configuring the Default Metric for Redistribution

Command	**default-metric** *metric*

Parameter Description	*metric*: Indicates the default metric of the OSPF redistributed route. The value ranges from 1 to 16,777,214.
Command Mode	OSPF routing process configuration mode
Usage Guide	The **default-metric**command must be used together with the **redistribute**command to modify the initial metrics of all redistributed routes. The **default-metric**command does not take effect on external routes that are injected to the OSPF routing domain by the **default-information originate** command.

Configuring the Maximum Metric

Command	**max-metric router-lsa** [**external-lsa** [*max-metric-value*]] [**include-stub**] [**on-startup**[*seconds*]] [**summary-lsa** [*max-metric-value*]]
Parameter Description	**router-lsa**: Sets the metrics of non-stub links in the Router LSA to the maximum value (0xFFFF). **external-lsa**: Allows a router to replace the metrics of external LSAs (including Type 5 and Type 7 LSAs) with the maximum metric. *max-metric-value*: Indicates the maximum metric of the LSA. The default value is 16711680. The value ranges from 1 to 16,777,215. **include-stub:** Sets the metrics of stub links in the Router LSA advertised by the router to the maximum value. **on-startup:** Allows a router to advertises the maximum metric when started. *seconds:* Indicates the interval at which the maximum metric is advertised. The default value is 600s. The value ranges from 5 to 86,400. **summary-lsa:** Allows a router to replace the metrics of summary LSAs (including Type 3 and Type 4 LSAs) with the maximum metric.
Command Mode	OSPF routing process configuration mode
Usage Guide	After the **max-metric router-lsa** command is executed, the metrics of the non-stub links in the Router LSAs generated by the router will be set to the maximum value (0xFFFF). If you cancel this configuration or the timer expires, the normal metrics of the links are restored. By default, if the **max-metric router-lsa** command is executed, the stub links still advertise common metrics, that is, the costs of outbound interfaces. If the **include-stub** parameter is configured, the stub links will advertise the maximum metric. If an ABR does not wish to transfer inter-area traffic, use the **summary-lsa** parameter to set the metric of the Summary LSA to the maximum metric. If an ASBR does not wish to transfer external traffic, use the **external-lsa** parameter to set the metric of the external LSA to the maximum metric. The **max-metric router-lsa** command is generally used in the following scenarios: Restart a device. After the device is restarted, IGP generally converges faster, and other devices attempt to forward traffic through the restarted device. ● Add a device to the network but the device is not used to transfer traffic. The device is added to the network. If a candidate path exists, the current device is not used to transfer traffic. If a candidate path does not exist, the current device is still used to transfer traffic. ● Delete a device gracefully from the network. After the **max-metric router-lsa** command is executed, the current device advertises the maximum metric among all metrics of routes. In this way, other devices on the network can

	select the standby path for data transmission before the device is shut down. In the earlier OSPF version (RFC1247 or earlier), the links with the maximum metric (0xFFFF) in the LSAs do not participate in the SPF computation, that is, no traffic is sent to routers that generate these LSAs.

Configuring RFC1583Compatibility

Command	**compatible rfc1583**
Parameter Description	N/A
Command Mode	OSPF routing process configuration mode
Usage Guide	When there are multiple paths to an ASBR or the forwarding address of an external route, RFC1583 and RFC2328 define different routing rules. If RFC1583 compatibilityis configured, a path in the backbone area or an inter-area path is preferentially selected. If RFC1583 compatibilityis not configured, a path in a non-backbone area is preferentially selected.

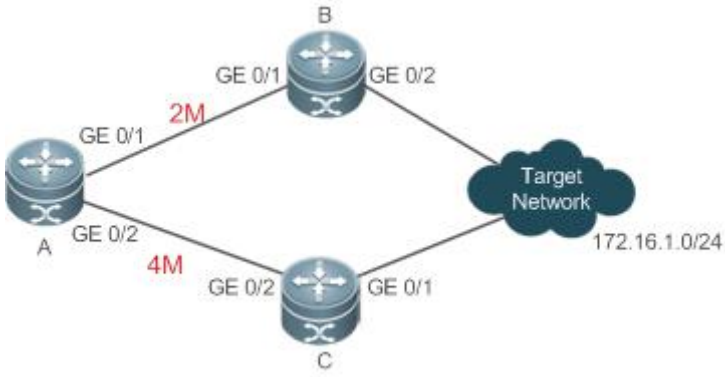
Configuring the AD

Command	**distance** { *distance* | **ospf** { [**intra-area***distance*] [**inter-area***distance*][**external** *distance*]} }
Parameter Description	*distance*: Indicates the AD of a route. The value ranges from 1 to 255. **intra-area** *distance*: Indicates the AD of an intra-area route. The value ranges from 1 to 255. **inter-area** *distance*: Indicates the AD of an inter-area route. The value ranges from 1 to 255. **external** *distance:* Indicates the AD of an external route. The value ranges from 1 to 255.
Command Mode	OSPF routing process configuration mode
Usage Guide	Use this command to specify different ADs for different types of OSPF routes.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 5.4.1 "Configuring OSPF Basic Functions."

Configuring the Cost of an Interface

Scenario	 **Remarks**: The interface IP addresses are as follows: A: GE0/1 192.168.1.1 GE0/2 192.168.2.1 B: GE0/1 192.168.1.2 GE0/2 192.168.3.2 C: GE0/1 192.168.4.2 GE0/2 192.168.2.2
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router A, configure the cost of each interface.
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip ospf cost 10 A(config)# interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)# ip ospf cost 20
Verification	On Router A, check the routing table. The next hop of the optimum path to 172.16.1.0/24 is Router B.
A	A# show ip route ospf O E2172.16.1.0/0 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1

Common Errors

- If the cost of an interface is set to 0 in the **ip ospf cost** command, a route computation error may occur. For example, a routing loop is obtained.

5.4.8 Enabling Authentication

Configuration Effect

- All routers connected to the OSPF network must be authenticated to ensure stability of OSPF and protect OSPF against intrusions.

Notes

- The OSPF basic functions must be configured.

- If authentication is configured for an area, the configuration takes effect on all interfaces that belong to this area.
- If authentication is configured for both an interface and the area to which the interface belongs, the configuration for the interface takes effect preferentially.

Configuration Steps

Configuring the Authentication Type of an Area

- (Optional) This configuration is recommended if the same authentication type should be used on all interfaces in the same area.
- This configuration is required if a router accesses a network that requires authentication.

Configuring the Authentication Type of an Interface

- (Optional) This configuration is recommended if the different authentication types should be used on different interfaces in the same area.
- This configuration is required if a router accesses a network that requires authentication.

Configuring a Plain Text Authentication Key for an Interface

- Optional.
- This configuration is required if a router accesses a network that requires plain text authentication.

Configuring an MD5 Authentication Key for an Interface

- (Optional) MD5 authentication features a high security, and therefore is recommended. You must configure either plain text authentication or MD5 authentication.
- This configuration is required if a router accesses a network that requires MD5 authentication.

Verification

- If routers are configured with different authentication keys, run the **show ip ospf neighbor** command to verify that there is no OSPF neighbor.
- If routers are configured with the same authentication key, run the **show ip ospf neighbor** command to verify that there are OSPF neighbors.

Related Commands

Configuring the Authentication Type of an Area

Command	**area** *area-id***authentication** [**message-digest**]
Parameter Description	*area-id*: Indicatesthe ID of the area where OSPF authentication is enabled. The area ID can be a decimal integer or an IP address. **message-digest**: Enables MD5 authentication.
Command Mode	OSPF routing process configuration mode
Usage Guide	The FSOS supports three authentication types: (1) Type 0: No authentication is required. If this command is not configured to enable OSPF authentication, the authentication type in the OSPF data packet is 0. (2) Type 1: The authentication type is plain text authentication if this command is configured but does not contain the

	message-digest parameter. (3) Type 3: The authentication type is MD5 authentication if this command is configured and contains the **message-digest** parameter. All routers in the same OSPF area must use the same authentication type. If authentication is enabled, the authentication key must be configured on interfaces that are connected to neighbors. You can run the interface configuration command **ip ospf authentication-key** to configure the plain text authentication key, or **ip ospf message-digest-key** to configure the MD5 authentication key.

Configuring the Authentication Type of an Interface

Command	**ip ospfauthentication** [**message-digest** | **null**]
Parameter Description	**message-digest**: Indicates that MD5 authentication is enabled on the current interface. **null**: Indicates that authentication is disabled.
Command Mode	Interface configuration mode
Usage Guide	If the **ip ospfauthentication** command does not contain any option, it indicates that plain text authentication is enabled. If you use the **no** form of the command to restore the default authentication mode, whether authentication is enabled is determined by the authentication type that is configured in the area to which the interface belongs. If the authentication type is set to null, authentication is disabled forcibly.When authentication is configured for both an interface and the area to which the interface belongs, the authentication type configured for the interface is used preferentially.

Configuring a Plain Text Authentication Key for an Interface

Command	**ip ospf authentication-key**[**0** |**7**]*key*
Parameter Description	**0**: Indicates that the key is displayed in plain text. **7**: Indicates that the key is displayed in cipher text. *key*: Indicates the key. The key is a string of up to eight characters.
Command Mode	Interface configuration mode
Usage Guide	The key configured by the **ip ospf authentication-key** command will be inserted to the headers of all OSPF packets. If the keys are inconsistent, two directly connected devices cannot set up the OSPF adjacency and therefore cannot exchange the routing information. Different keys can be configured for different interface, but all routers connected to the same physical network segment must be configured with the same key. You can enable or disable authentication in an OSPF area by running the **areaauthentication** command in OSPF routing process configuration mode. You can also enable authentication on an individual interface by running the **ip ospf authentication** command in interface configuration mode. When authentication is configured for both an interface and the area to which the interface belongs, the authentication type configured for the interface is used preferentially.

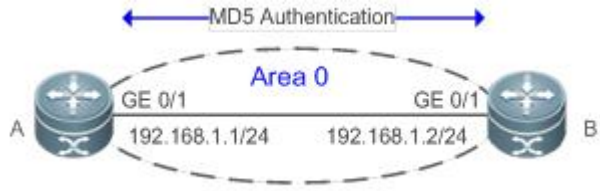
Configuring an MD5 Authentication Key for an Interface

Command	**ip ospf message-digest-key** *key-id* **md5**[**0** |**7**]*key*
Parameter Description	*key-id:* Indicates the key ID. The value ranges from 1 to 255. **0**: Indicates that the key is displayed in plain text. **7**: Indicates that the key is displayed in cipher text.

	key: Indicates the key. The key is a string of up to 16 characters.
Command Mode	Interface configuration mode
Usage Guide	The key configured by the **ip ospf message-digest-key** command will be inserted to the headers of all OSPF packets. If the keys are inconsistent, two directly connected devices cannot set up the OSPF adjacency and therefore cannot exchange the routing information. Different keys can be configured for different interface, but all routers connected to the same physical network segment must be configured with the same key. The same key ID on neighbor routers must correspond to the same key. You can enable or disable authentication in an OSPF area by running the **area authentication** command in OSPF routing process configuration mode. You can also enable authentication on an individual interface by running the **ip ospf authentication** command in interface configuration mode. When authentication is configured for both an interface and the area to which the interface belongs, the authentication type configured for the interface is used preferentially. The FSOS software supports smooth modification of the MD5 authentication key. A new MD5 authentication key must be first added before the old key can be deleted. When an OSPF MD5 authentication key is added to a router, the router determines that other routers do not use the new key yet and therefore uses different keys to send multiple OSPF packets until it confirms that the new key has been configured on neighbors. After configuring the new key all routers, you can delete the old key.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 5.4.1 "Configuring OSPF Basic Functions."

Scenario	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Configure the authentication type and MD5 authentication key on all routers.
A	A# configure terminal A(config)#router ospf 1 A(config-router)#area 0 authentication message-digest A(config-router)#exit A(config)#interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#ip ospf message-digest-key 1 md5 hello

B	B# configure terminal B(config)#router ospf 1 B(config-router)#area 0 authentication message-digest B(config-router)#exit B(config)#interface GigabitEthernet 0/3 B(config-if-GigabitEthernet 0/3)#ip ospf message-digest-key 1 md5 hello
Verification	On Router A and Router B, verify that the OSPF neighbor status is correct.
A	A#show ip ospf neighbor OSPF process 1, 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.2 1 Full/DR 00:00:32 192.168.1.2 GigabitEthernet 0/1
B	A#show ip ospf neighbor OSPF process 1, 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.1 1 Full/DR 00:00:32 192.168.1.1 GigabitEthernet 0/1

Common Errors

- The authentication modes configured on routers are inconsistent.
- The authentication keys configured on routers are inconsistent.

5.4.9 Enabling Overflow

Configuration Effect

- New routes are not loaded to routers when the router memory is insufficient.
- New routes are not loaded to routers when the usage of the database space reaches the upper limit.

Notes

- The OSPF basic functions must be configured.
- After a router enters the overflow state, you can run the **clear ip ospf process** command, or stop and then restart the OSPF to exit the overflow state.

Configuration Steps

↘ Configuring the Memory Overflow Function

- Optional.
- This configuration is recommended if a large number of routes exist in the domain and may cause insufficiency of the router memory.

Configuring the Database Overflow Function

- Optional.
- This configuration is recommended if a large number of routes exist in the domain and may cause insufficiency of the router memory.

Configuring the External LSA Database Overflow Function

- Optional.
- This configuration is recommended if the ASBR introduces a large number of external routes and the router memory may be insufficient.

Verification

- After the memory becomes insufficient, add new routers to the network, and run the **show ip route** command to verify that new routes are not loaded.
- After the usage of the database space reaches the upper limit, add new routers to the network, and run the **show ip route** command to verify that new routes are not loaded.

Related Commands

Configuring the Memory Overflow Function

Command	**overflow memory-lack**
Parameter Description	N/A
Command Mode	OSPF routing process configuration mode
Usage Guide	The OSPF process enters the overflow state to discard newly-learned external routes. This behavior can effectively ensure that the memory usage does not increase. After the overflow function is enabled, the OSPF process enters the overflow state and discards newly-learned external routes, which may cause a routing loop on the entire network. To reduce the occurrence probability of this problem, OSPF generates a default route to the null interface, and this route always exists in the overflow state. You can run the **clear ip ospf process** command to reset the OSPF process so that the OSPF process can exit the overflow state. You can use the **no** form of the command to prevent the OSPF process from entering the overflow state when the memory is insufficient. This, however, may lead to over-consumption of the memory resource, after which the OSPF process will stop and delete all the learned routes.

Configuring the Database Overflow Function

Command	**overflow database***number* [**hard** | **soft**]
Parameter Description	*number*: Indicates the maximum number of LSAs. The value ranges from 1 to 4,294,967,294. **hard**: Indicates that the OSPF process will be stopped if the number of LSAs exceeds the limit. **soft:** Indicates that a warning will be generated if the number of LSAs exceeds the limit.
Command Mode	OSPF routing process configuration mode
Usage Guide	If the number of LSAs exceeds the limit, use the **hard** parameter if the OSPF process should be stopped, and use the **soft** parameter if a warning should be generated without stopping the OSPF process.

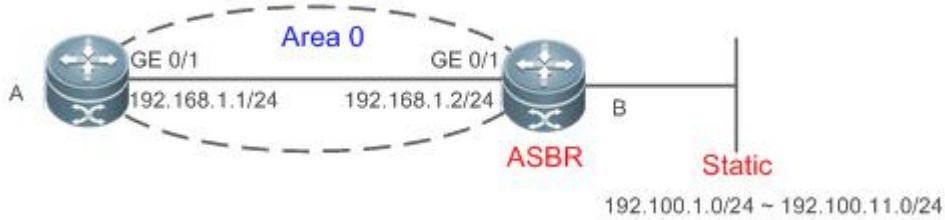
Configuring the External LSA Database Overflow Function

Command	**overflow database external** *max-dbsize wait-time*
Parameter Description	*max-dbsize*: Indicates the maximum number of external LSAs. This value must be the same on all routers in the same AS. The value ranges from 0 to 2,147,483,647. *wait-time*: Indicates the waiting time after a router in overflow state attempts to restore the normal state. The value ranges from 0 to 2,147,483,647.
Command Mode	OSPF routing process configuration mode
Usage Guide	When the number of external LSAs of a router exceeds the configured **max-dbsize**, the router enters the overflow state. In this state, the router no longer loads external LSAs and deletes external LSAs that are generated locally. After *wait-time* elapses, the device restores the normal state, and loads external LSAs again. When using the overflow function, ensure that the same **max-dbsize** is configured on all routers in the OSPF backbone area and common areas; otherwise, the following problems may occur: Inconsistent LSDBs throughout network are inconsistent, and the failure to achieve the full adjacency Incorrect routes, including routing loops Frequent retransmission of AS external LSAs

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 5.4.1 "Configuring OSPF Basic Functions."

Configuring the External LSA Database Overflow Function

Scenario	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router B, configure redistribution and introduce external static routes. ● On Router B, configure the maximum number of external LSAs.
B	B# configure terminal B(config)# router ospf 1 B(config-router)# redistribute static subnets

A	A# configure terminal A(config)# router ospf 1 A(config-router)# overflow database external 10 3
Verification	On Router B, configure 11 static routes (192.100.1.0/24 to 192.100.11.0/24). On Router A, verify that only 10 static routes are loaded.
A	A# show ip route ospf O E2 192.100.1.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.2.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.3.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.4.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.5.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.6.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.7.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.8.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.9.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.10.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1

Common Errors

- The OSPF adjacency is abnormal because the maximum number of LSAs is inconsistent on different routers.

5.4.10 Modifying the Maximum Number of Concurrent Neighbors

Configuration Effect

- Control the maximum number of concurrent neighbors on the OSPF process to ease the pressure on the device.

Notes

- The OSPF basic functions must be configured.

Configuration Steps

Configuring the Maximum Number of Concurrent Neighbors on the OSPF Process

- (Optional) This configuration is recommended if you wish to set up the OSPF adjacencymore quickly when a router is connected with a lot of other routers.
- This configuration is performed on a core router.

Verification

- Run the **show ip ospf neighbor** command to display the number of neighbors that are concurrently interacting with the OSPF process.

Related Commands

Configuring the Maximum Number of Concurrent Neighbors on the Current Process

Command	**max-concurrent-dd***number*
Parameter Description	*number:* Specifies the maximum number of neighbors that are concurrently interacting with the OSPF process. The value ranges from 1 to 65,535.
Command Mode	OSPF routing process configuration mode
Usage Guide	When the performance of a router is affected because the router exchanges data with multiple neighbors, you can configure this command to restrict the maximum of neighbors with which one OSPF process can concurrently initiates or accepts interaction.

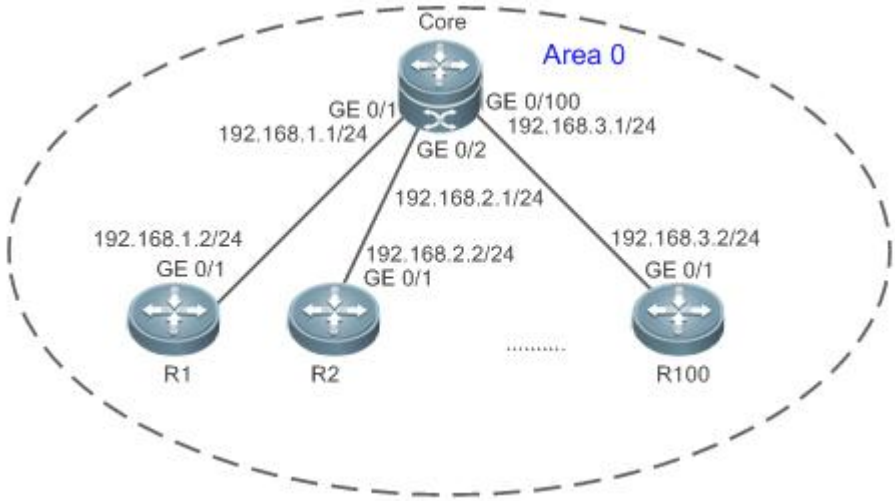
Configuring the Maximum Number of Concurrent Neighbors on All Processes

Command	**router ospf max-concurrent-dd***number*
Parameter Description	*number:* Specifies the maximum number of neighbors that are concurrently interacting with the OSPF process. The value ranges from 1 to 65,535.
Command Mode	Global configuration mode
Usage Guide	When the performance of a router is affected because the router exchanges data with multiple neighbors, you can configure this command to restrict the maximum of neighbors with which all OSPF processes can concurrently initiate or accept interaction.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 5.4.1 "Configuring OSPF Basic Functions."

Configuring the Maximum Number of Concurrent Neighbors on the OSPF Process

Scenario	

Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On the router Core, set the maximum number of concurrent neighbors to 4.
Core	Core# configure terminal Core(config)# router ospf max-concurrent-dd 4
Verification	On therouter Core, check the neighbor status and verify that at most eight neighbors concurrently interact with the OSPF process.

5.4.11 Disabling Source Address Verification

Configuration Effect

- The unicast routing service can be provided even if the interface IP addresses of neighbor routers are not in the same network segment.

Notes

- The OSPF basic functions must be configured.
- Source address verification cannot be disabled on a broadcast or NBMA network.

Configuration Steps

Disabling Source Address Verification

- (Optional) This configuration is mandatory if an adjacency should be set up between routers with interface IP addresses in different network segments.
- This configuration is performed on routers with interface IP addresses in different network segments.

Verification

- An adjacency can be set up between routers in different network segments.

Related Commands

Disabling Source Address Verification

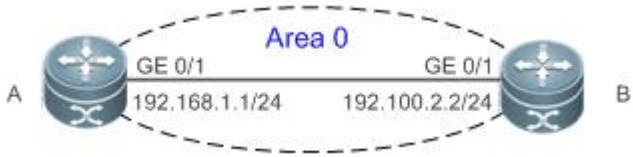
Command	ip ospf source-check-ignore
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Generally, the source address of a packet received by OSPF is in the same network segment as the receiving interface. The addresses at both ends of a P2P link are configured separately and are not necessarily in the same network segment. In this scenario, as the peer address information will be notified during the P2P link negotiation process, OSPF checks whether the source address of the packet is the address advertised by the peer during negotiation. If not, OSPF

	determines that the packet is invalid and discards this packet. In particular, OSPF does not verify the address of an unnumbered interface. In some scenarios, the source address may not meet the preceding requirement, and therefore OSPF address verification fails. For example, the negotiated peer address cannot be obtained on a P2P link. In this scenario, source address verification must be disabled to ensure that the OSPF adjacency can be properly set up.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 5.4.1 "Configuring OSPF Basic Functions."

Disabling Source Address Verification

Scenario	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Set the network types of interfaces on all routers to P2P. ● Disable source address verification on all routers.
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip ospf network point-to-point A(config-if-GigabitEthernet 0/1)# ip ospf source-check-ignore
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip ospf network point-to-point B(config-if-GigabitEthernet 0/1)# ip ospf source-check-ignore
Verification	On Router A, verify that the OSPF neighbor information is correct.
A	A# show ip ospfneighbor OSPF process 1, 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.100.2.2 1 Full/- 00:00:34 192.100.2.2 GigabitEthernet 0/1

5.4.12 Disabling MTU Verification

Configuration Effect

- The unicast routing service can be provided even if the MTUs of interfaces on neighbor routers are different.

Notes

- The OSPF basic functions must be configured.

Configuration Steps

Disabling MTU Verification

- (Optional) MTU verification is disabled by default. You are advised to retain the default configuration.
- This configuration is performed on two routers with different interface MTUs.

Verification

The adjacency can be set up between routers with different MTUs.

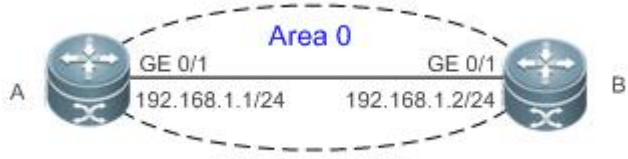
Related Commands

Disabling MTU Verification

Command	ip ospf mtu-ignore
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	On receiving the database description packet, OSPF checks whether the MTU of the interface on the neighbor is the same as the MTU of its own interface. If the interface MTU specified in the received database description packet is greater than the MTU of the local interface, the adjacency cannot be set up. To resolve this problem, you can disable MTU verification.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 5.4.1 "Configuring OSPF Basic Functions."

Scenario	

Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Configure different MTUs for interfaces on two routers. ● Disable MTU verification on all routers. (By default, the function of disabling MTU verification is enabled.)
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip mtu 1400 A(config-if-GigabitEthernet 0/1)# ip ospf mtu-ignore
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip mtu 1600 B(config-if-GigabitEthernet 0/1)# ip ospf mtu-ignore
Verification	● On Router A, verify that the OSPF neighbor information is correct.
A	A# show ip ospfneighbor OSPF process 1, 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.2 1 Full/DR 00:00:34 192.168.1.2 GigabitEthernet 0/1

5.4.13 Enabling Two-Way Maintenance

Configuration Effect

- Non-Hello packets can also be used to maintain the adjacency.

Notes

- The OSPF basic functions must be configured.

Configuration Steps

Enabling Two-Way Maintenance

- (Optional) This function is enabled by default. You are advised to retain the default configuration.
- This configuration is performed on all routers.

Verification

Non-Hello packets can also be used to maintain the adjacency.

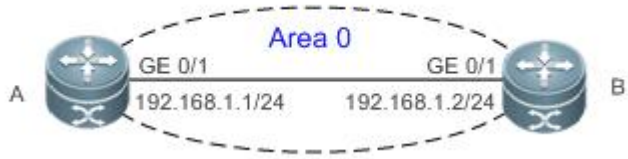
Related Commands

Enabling Two-Way Maintenance

Command	two-way-maintain
Parameter Description	N/A
Command Mode	OSPF routing process configuration mode
Usage Guide	On a large network, a lot of packets may be sent or received, occupying too much CPU and memory. As a result, some packets are delayed or discarded. If the processing time of Hello packets exceeds the dead interval, the adjacency will be destroyed due to timeout.If the two-way maintenance function is enabled, in addition to the Hello packets, the DD, LSU, LSR, and LSAck packets can also be used to maintain the bidirectional communication between neighbors when a large number of packets exist on the network. This prevents termination of the adjacency caused by delayed or discarded Hello packets.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 5.4.1 "Configuring OSPF Basic Functions."

Scenario	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router A, enable the two-way maintenance function. (This function is enabled by default.)
A	A# configure terminal A(config)#routerospf 1 A(config-router)#two-way-maintain
Verification	When the adjacency is being set up, Router A checks the neighbor dead interval and updates the dead interval without waiting for Router B to send a Hello packet.
A	A# show ip ospfneighbor OSPF process 1, 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.2 1 Full/BDR 00:00:40 192.168.1.2 GigabitEthernet 0/1

5.4.14 Enabling GR

Configuration Effect

- When a distributed router switches services from the active board to the standby board, data forwarding continues and is not interrupted.
- When the OSPF process is being restarted, data forwarding continues and is not interrupted.

Notes

- The OSPF basic functions must be configured.
- The neighbor router must support the GR helper function.
- The grace period cannot be shorter than the neighbor dead time of the neighbor router.

Configuration Steps

Configuring the OSPF GR Function

- (Optional) This function is enabled by default. You are advised to retain the default configuration.
- This configuration is performed on all routers.

Configuring the OSPF GR Helper Function

- (Optional) This function is enabled by default. You are advised to retain the default configuration.
- This configuration is performed on all routers.

Verification

- When a distributed router switches services from the active board to the standby board, data forwarding continues and is not interrupted.
- When the OSPF process is being restarted, data forwarding continues and is not interrupted.

Related Commands

Configuring the OSPF GR Function

Command	**graceful-restart** [**grace-period** *grace-period* | **inconsistent-lsa-checking**]
Parameter Description	**grace-period** *grace-period*: Indicates the grace period, which is the maximum time from occurrence of an OSPF failure to completion of the OSPF GR. The value of the graceperiod varies from 1s to 1800s. The default value is 120s. **inconsistent-lsa-checking**: Enables topological change detection. If any topological change is detected, OSPF exits the GR process to complete convergence.After GR is enabled, topological change detection is enabled by default.
Command Mode	OSPF routing process configuration mode
Usage Guide	The GR function is configured based on the OSPF process. You can configure different parameters for different OSPF processes based on the actual conditions. This command is used to configure the GR restarter capability of a device. The grace period is the maximum time of the entire GR process, during which link status is rebuilt so that the original state of the OSPF process is restored. After the grace period expires, OSPF exits the GR state and performs common OSPF operations.

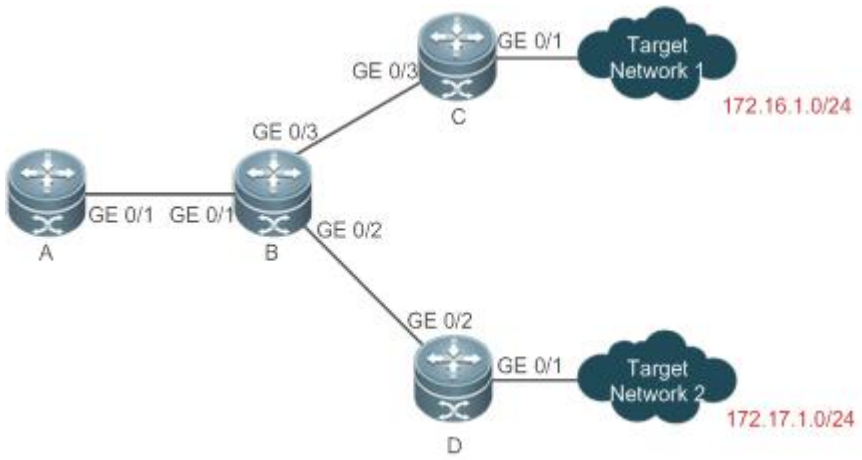
	Run the**graceful-restart** command to set the grace period to 120s. The **graceful-restart grace-period** command allows you to modify the grace period explicitly. The precondition for successful execution of GR and uninterrupted forwarding is that the topology remains stable.If the topology changes, OSPF quickly converges without waiting for further execution of GR, thus avoiding long-time forwarding black-hole. Disabling topology detection: If OSPF cannot converge in time when thetopology changes during the hot standby process, forwarding black-hole may appear in a long time. Enabling topology detection: Forwarding may be interrupted when topology detection is enabled, but the interruption time is far shorter than that when topology detection is disabled. In most cases, it is recommended that topology detection be enabled. In special scenarios, topology detection can be disabled if the topology changes after the hot standby process, but it can be ensured that the forwarding black-hole will not appearin a long time. This can minimize the forwarding interruption time during the hot standby process. If the Fast Hello function is enabled, the GR function cannot be enabled.

Configuring the OSPF GR Helper Function

Command	**graceful-restart helper** { **disable** | **strict-lsa-checking** | **internal-lsa-checking**}
Parameter Description	**disable**: Prohibits a device from acting as a GR helper for another device. **strict-lsa-checking**: Indicates that changes in Type 1 to Type 5 and Type 7 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network changes, the device will stop acting as the GR helper. **internal-lsa-checking:** Indicates that changes in Type 1 to Type 3 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network changes, the device will stop acting as the GR helper.
Command Mode	OSPF routing process configuration mode
Usage Guide	This command is used to configure the GR helper capability of a router. When a neighbor router implements GR, it sends a Grace-LSA to notify all neighbor routers. If the GR helper function is enabled on the local router, the local router becomes the GR helper on receiving the Grace-LSA, and helps the neighbor to complete GR. The **disable** option indicates that GR helper is not provided for any device that implements GR. After a device becomes the GR helper, the network changes are not detected by default. If any change takes place on the network, the network topology converges after GR is completed. If you wish that network changes can be quickly detected during the GR process, you can configure **strict-lsa-checking** to check Type 1 to 5 and Type 7 LSAs that indicate the network information or **internal-lsa-checking** to check Type 1 to 3 LSAs that indicate internal routes of the AS domain. When the network scale is large, it is recommended that you disable the LSA checking options (**strict-lsa-checking** and **internal-lsa-checking**) because regional network changes may trigger termination of GR and consequently reduce the convergence of the entire network.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 5.4.1 "Configuring OSPF Basic Functions."

Scenario	 **Remarks**: The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 B: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 GE 0/3 192.168.3.1 C: GE 0/1 192.168.4.2 GE 0/3 192.168.3.2 D: GE 0/1 192.168.5.2 GE 0/2 192.168.2.2
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router A, Router C, and Router D, enable the GR helper function. (This function is enabled by default.) ● On Router B, enable the GR function.
B	B# configure terminal B(config)# router ospf1 B(config-router)# graceful-restart
Verification	● Trigger a hot standby switchover on Router B, and verify that the routing tables of destination networks 1 and 2 remain unchanged on Router A during the switchover. ● Trigger a hot standby switchover on Router B, ping destination network 1 from Router A, and verify that data forwarding is not interrupted during the switchover.

Common Errors

- Traffic forwarding is interrupted during the GR process because the configured grace period is shorter than the neighbor dead time of the neighbor router.

5.4.15 Configuring the Network Management Function

Configuration Effect

- Use the network management software to manage OSPF parameters and monitor the OSPF running status.

Notes

- The OSPF basic functions must be configured.
- You must enable the MIB function of the SNMP-Server before enabling the OSPF MIB function.
- You must enable the Trap function of the SNMP-Server before enabling the OSPF Trap function.
- You must enable the logging function of the device before outputting the OSPF logs.

Configuration Steps

Binding the MIB with the OSPF Process

- (Optional) This configuration is required if you want to use the network management software to manage parameters of a specified OSPF process.
- This configuration is performed on all routers.

Enabling the Trap Function

- (Optional) This configuration is required if you want to use the network management software to monitor the OSPF running status.
- This configuration is performed on all routers.

Configuring the Logging Function

- (Optional) This function is enabled by default. You are advised to retain the default configuration. If you want to reduce the log output, disable this function.
- This configuration is performed on all routers.

Verification

- Use the network management software to manage the OSPF parameters.
- Use the network management software to monitor the OSPF running status.

Related Commands

Binding the MIB with the OSPF Process

Command	enable mib-binding
Parameter Description	N/A
Command Mode	OSPF routing process configuration mode
Usage Guide	The OSPFv2 MIB does not have the OSPFv2 process information. Therefore, you must perform operations on a single OSPFv2 process through SNMP. By default, the OSPFv2 MIB is bound with the OSPFv2 process with the smallest process ID, and all user operations take effect on this process. If you wish to perform operations on a specified OSPFv2 through SNMP, run this command to bind the MIB with the process.

Enabling the Trap Function

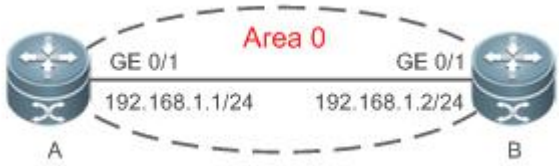
Command	**enable traps**[**error** [**IfAuthFailure** | **IfConfigError** | **IfRxBadPacket** | **VirtIfAuthFailure** | **VirtIfConfigError** | **VirtIfRxBadPacket**] | **lsa** [**LsdbApproachOverflow** | **LsdbOverflow** | **MaxAgeLsa** | **OriginateLsa**] | **retransmit** [**IfTxRetransmit** | **VirtIfTxRetransmit**] | **state-change**[**IfStateChange** | **NbrRestartHelperStatusChange** | **NbrStateChange** | **NssaTranslatorStatusChange** | **RestartStatusChange** | **VirtIfStateChange** | **VirtNbrRestartHelperStatusChange**| **VirtNbrStateChange**]]
Parameter Description	**IfAuthFailure**: Indicates that an interface authentication failure occurs. **IfConfigError:** Indicates that an interface parameter configuration error occurs. **IfRxBadPacket:** Indicates that the interface receives a bad packet. **IfRxBadPacket:** Indicates that the interface receives a bad packet. **VirtIfAuthFailure:** Indicates that a virtual interface authentication failure occurs. **VirtIfConfigError:** Indicates that a virtual interface parameter configuration error occurs. **VirtIfRxBadPacket:** Indicates that the virtual interface receives a bad packet. **LsdbApproachOverflow:** Indicates that the number of external LSAs has reached 90% of the upper limit. **LsdbOverflow:** Indicates that the number of external LSAs has reached the upper limit. **MaxAgeLsa:** Indicates that the LSA aging timer expires. **OriginateLsa:** Indicates that a new LSA is generated. **IfTxRetransmit:** Indicates that a packet is retransmitted on the interface. **VirtIfTxRetransmit:** Indicates that a packet is retransmitted on the virtual interface. **IfStateChange:** Indicates that interface state changes. **NbrRestartHelperStatusChange:**Indicates that the state of the neighbor GR process changes. **NbrStateChange:** Indicates that the neighbor state changes. **NssaTranslatorStatusChange:** Indicates that the NSSA translation state changes. **RestartStatusChange:** Indicates that the GR state of the local device changes. **VirtIfStateChange:** Indicates that the virtual interface state changes. **VirtNbrRestartHelperStatusChange:** Indicates that the GR state of the virtual neighbor changes. **VirtNbrStateChange:** Indicates that the virtual neighbor state changes.
Command Mode	OSPF routing process configuration mode
Usage Guide	The function configured by this command is restricted by the **snmp-server** command. You can configure **snmp-server enable traps ospf** and then **enable traps** command before the corresponding OSPF traps can be correctly sent out. This command is not restricted by the MIB bound with the process. The trap function can be enabled concurrently for different processes.

Configuring the Logging Function

Command	**log-adj-changes**[**detail**]
Parameter Description	**detail**: Records all status change information.
Command Mode	OSPF routing process configuration mode
Usage Guide	N/A

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 5.4.1 "Configuring OSPF Basic Functions."

Scenario	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Bind the MIB with the OSPF process on Router A. ● Enable the trap function on Router A.
A	A# configure terminal A(config)# snmp-server host 192.168.2.2 traps version 2c public A(config)# snmp-server community public rw A(config)# snmp-server enable traps A(config)# router ospf 10 A(config-router)# enable mib-binding A(config-router)# enable traps
Verification	Use the MIB tool to read and set the OSPF parameters and display the OSPF running status.

Common Errors

Configurations on the SNMP-Server are incorrect. For example, the MIB or trap function is not enabled.

5.4.16 Modifying Protocol Control Parameters

Configuration Effect

Modify protocol control parameters to change the protocol running status.

Notes

- The OSPF basic functions must be configured.
- The neighbor dead time cannot be shorter than the Hello interval.

Configuration Steps

Configuring the Hello Interval

- (Optional) You are advised to retain the default configuration.
- This configuration is performed on routers at both end of a link.

Configuring the Dead Interval

- (Optional) You are advised to retain the default configuration. This configuration can be adjusted if you wish to accelerate OSPF convergence when a link fails.
- This configuration is performed on routers at both end of a link.

Configuring LSU Retransmission Interval

- (Optional) You are advised to adjust this configuration if a lot of routes exist in the user environment and network congestion is serious.

Configuring the LSA Generation Time

- (Optional) You are advised to retain the default configuration.

Configuring the LSA Group Refresh Time

- (Optional) You are advised to retain the default configuration. This configuration can be adjusted if a lot of routes exist in the user environment.
- This configuration is performed on an ASBR or ABR.

Configuring LSA Repeated Receiving Delay

- (Optional) You are advised to retain the default configuration.

Configuring the SPF Computation Delay

- (Optional) This configuration can be adjusted if network flapping frequently occurs.

Configuring the Inter-Area Route Computation Delay

- (Optional) You are advised to retain the default configuration.
- This configuration is performed on all routers.

Configuring the External Route Computation Delay

- (Optional) You are advised to retain the default configuration.
- This configuration is performed on all routers.

Verification

Run the **show ip ospf**and**show ip ospf neighbor** commands to display the protocol running parameters and status.

Related Commands

Configuring the Hello Interval

Command	**ip ospf hello-interval***seconds*
Parameter Description	*seconds*: Indicates the interval at which OSPF sends the Hello packet. The unit is second. The value ranges from 1 to 65,535.
Command Mode	Interface configuration mode
Usage Guide	The Hello interval is contained in the Hello packet. A shorter Hello interval indicates that OSPF can detect topological changes more quickly, but the network traffic increases. The Hello interval must be the same on all routers in the same

	network segment. If you want to manually modify the neighbor dead interval, ensure that the neighbor dead interval is longer than the Hello interval.

Configuring the Dead Interval

Command	**ip ospf dead-interval** *seconds*
Parameter Description	*seconds*: Indicates the time that the neighbor is declared lost. The unit is second. The value ranges from 0 to 2,147,483,647.
Command Mode	Interface configuration mode
Usage Guide	The OSPF dead interval is contained in the Hello packet. If OSPF does not receive a Hello packet from a neighbor within the dead interval, it declares that the neighbor is invalid and deletes this neighbor record form the neighbor list. By default, the dead interval is four times the Hello interval. If the Hello interval is modified, the dead interval is modified automatically. When using this command to manually modify the dead interval, pay attention to the following issues: 1. The dead interval cannot be shorter than the Hello interval. 2. The dead interval must be the same on all routers in the same network segment.

Configuring the LSU Transmission Delay

Command	**ip ospf transmit-delay***seconds*
Parameter Description	*seconds*: Indicates the LSU transmission delay on the OSPF interface. The unit is second. The value ranges from 0 to 65,535.
Command Mode	Interface configuration mode
Usage Guide	Before an LSU packet is transmitted, the Age fields in all LSAs in this packet will increase based on the amount specified by the **ip ospf transmit-delay** command. Considering the transmit and line propagation delays on the interface, you need to set the LSU transmission delay to a greater value for a low-speed line or interface. The LSU transmission delay of a virtual link is defined by the **transmit-delay** parameter in the **area virtual-link** command. If the value of the Age field of an LSA reaches 3600, the packet will be retransmitted or a retransmission will be requested. If the LSA is not updated in time, the expired LSA will be deleted from the LSDB.

Configuring LSU Retransmission Interval

Command	**ip ospf retransmit-interval***seconds*
Parameter Description	*seconds*: Indicates the LSU retransmission interval. The unit is second. The value ranges from 1 to 65,535. This interval must be longer than the round-trip transmission delay of data packets between two neighbors.
Command Mode	Interface configuration mode
Usage Guide	After a router finishes sending an LSU packet, this packet is still kept in the transmit buffer queue. If an acknowledgment from the neighbor is not received within the time defined by the **ip ospf retransmit-interval** command, the router retransmits the LSU packet. The retransmission delay can be set to a greater value on a serial line or virtual link to prevent unnecessary retransmission. The LSU retransmission delay of a virtual link is defined by the **retransmit-interval** parameter in the **area virtual-link** command.

Configuring the LSA Generation Time

Command	**timers throttle lsa all** *delay-time hold-time max-wait-time*
Parameter Description	*delay-time*: Indicates the minimum delay for LSA generation. The first LSA in the database is always generated instantly. The value ranges from 0 to 600,000. The unit is ms. *hold-time*: Indicates the minimum interval between the first LSA update and the second LSA update. The value ranges from 1 to 600,000. The unit is ms. *max-wait-time*: Indicates the maximum interval between two LSA updates when the LSA is updated continuously. This interval is also used to determine whether the LSA is updated continuously. The value ranges from 1 to 600,000. The unit is ms.
Command Mode	OSPF routing process configuration mode
Usage Guide	If a high convergence requirement is raised when a link changes, you can set **delay-time** to a smaller value. You can also appropriately increase values of the preceding parameters to reduce the CPU usage. When configuring this command, the value of **hold-time** cannot be smaller than the value of **delay-time,** and the value of **max-wait-time** cannot be smaller than the value of **hold-time**.

Configuring the LSA Group Refresh Time

Command	**timers pacinglsa-group** *seconds*
Parameter Description	*seconds*: Indicates the LSA group pacing interval. The value ranges from 10 to 1,800. The unit is second.
Command Mode	OSPF routing process configuration mode
Usage Guide	Every LSA has a time to live (LSA age). When the LSA age reaches 1800s, a refreshment is needed to prevent LSAs from being cleared because their ages reaching the maximum. If LSA update and aging computation are performed for every LSA, the device will consume a lot of CPU resources. In order to use CPU resources effectively, you can refresh LSAs by group on the device. The interval of group refreshment is called group pacing interval. The group refreshment operation is to organize the LSAs generated within a group pacing interval into a group and refresh the group as a whole. If the total number of LSAs does not change, a larger group pacing interval indicates that more LSAs need to be processed after timeout. To maintain the CPU stability, the number of LSAs processes upon each timeout cannot be too large. If the number of LSAs is large, you are advised to reduce the group pacing interval. For example, if there are 1000 LSAs in the database, you can reduce the pacing interval; if there are 40 to 100 LSAs, you can set the pacing interval to 10-20 minutes.

Configuring the LSA Group Refresh Interval

Command	**timers pacing lsa-transmit** *transmit-time transmit-count*
Parameter Description	*transmit-time*: Indicates the LSA group transmission interval. The value ranges from 10 to 1,000. The unit is ms. *transmit-count*: Indicates the number of LS-UPD packets in a group. The value ranges from 1 to 200.
Command Mode	OSPF routing process configuration mode
Usage Guide	If the number of LSAs is large and the device load is heavy in an environment, properly configuring **transimit-time** and **transimit-count** can limit the number of LS-UPD packets flooded on a network. If the CPU usage is not high and the network bandwidth load is not heavy, reducing the value of **transimit-time** and increasing the value of **transimit-count** can accelerate the environment convergence.

Configuring LSA Repeated Receiving Delay

Command	**timers lsa arrival** *arrival-time*
Parameter Description	*arrival-time*: Indicates the delay after which the same LSA is received. The value ranges from 0 to 600,000. The unit is ms.
Command Mode	OSPF routing process configuration mode
Usage Guide	No processing is performed if the same LSA is received within the specified time.

Configuring the Inter-Area Route Computation Delay

Command	**timers throttle route inter-area** *ia-delay*
Parameter Description	*ia-delay*: Indicates the inter-area route computation delay. The unit is ms. The value ranges from 0 to 600,000.
Command Mode	OSPF routing process configuration mode
Usage Guide	This delay cannot be modified if strict requirements are raised for the network convergence time.

Configuring the External Route Computation Delay

Command	**timers throttle route ase** *ase-delay*
Parameter Description	*ase-delay*: Indicates the external route computation delay. The unit is ms. The value ranges from 0 to 600,000.
Command Mode	OSPF routing process configuration mode
Usage Guide	This delay cannot be modified if strict requirements are raised for the network convergence time.

Configuring the SPF Computation Delay

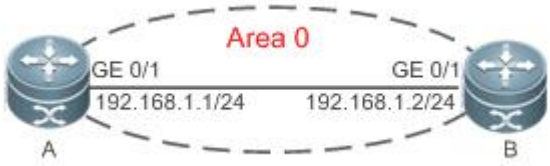
Command	**timers throttle spf** *spf-delay spf-holdtime spf-max-waittime*
Parameter Description	*spf-delay*: Indicates the SPF computation delay. The unit is ms. The value ranges from 1 to 600,000. When detecting a topological change, the OSPF routing process triggers the SPF computation at least after **spf-delay** elapses. *spf-holdtime*: Indicates the minimum interval between two SPF computations. The unit is ms. The value ranges from 1 to 600,000. *spf-max-waittime*: Indicates the maximum interval between two SPF computations. The unit is ms. The value ranges from 1 to 600,000. *number*: indicates the metric of the summarized route.
Command Mode	OSPF routing process configuration mode
Usage Guide	**spf-delay** indicates the minimum time between the occurrence of the topological change and the start of SPF computation. **spf-holdtime** indicates the minimum interval between the first SPF computation and the second SPF computation. After that, the interval between two SPF computations must be at least twice of the previous interval. When the interval reaches **spf-max-waittime**, the interval cannot increase again. If the interval between two SPF computations already exceeds the required minimum value, the interval is computed by starting from **spf-holdtime**. You can set **spf-dela**y and **spf-holdtime** to smaller values to accelerate topology convergence, and set **spf-max-waittime** to a larger value to reduce SPF computation. Flexible settings can be used based on stability of the network topology. Compared with the **timers spf** command, this command supports more flexible settings to accelerate the convergence speed of SPF computation and further reduce the system resources consumed by SPF computation when the topology

	continuously changes. Therefore, you are advised to use the **timers throttle spf** command for configuration. 1. The value of **spf-holdtime** cannot be smaller than the value of **spf-delay**; otherwise, **spf-holdtime** will be automatically set to the value of **spf-delay**. 2. The value of **spf-max-waittime** cannot be smaller than the value of **spf-holdtime**; otherwise, **spf-max-waittime** will be automatically set to the value of **spf-holdtime**. 3. The configurations of **timers throttle spf** and **timers spf** are mutually overwritten. 4. When both **timers throttle spf** and **timers spf** are not configured, the default values of **timers throttle spf** prevail.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 5.4.1 "Configuring OSPF Basic Functions."

Configuring the Hello Interval and Dead Interval

Scenario	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Configure the Hello interval and dead interval on all routers.
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip ospf hello-interval 15 A(config-if-GigabitEthernet 0/1)# ip ospf dead-interval 50
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip ospf hello-interval 15 A(config-if-GigabitEthernet 0/1)# ip ospf dead-interval 50
Verification	Check the interface parameters on Router A. Verify that the Hello interval is 10s and the dead interval is 50s.

A	A# show ip ospf interface GigabitEthernet 0/1 is up, line protocol is up Internet Address 192.168.1.1/24, Ifindex 2, Area 0.0.0.0, MTU 1500 Matching network config: 192.168.1.0/24 Process ID 1, Router ID 192.168.1.2, Network Type POINTOMULTIPOINT, Cost: 1 Transmit Delay is 1 sec, State Point-To-Point Timer intervals configured, Hello 15, Dead 50, Wait 40, Retransmit 5 Hello due in 00:00:02 Neighbor Count is 1, Adjacent neighbor count is 0 Crypt Sequence Number is 4787 Hello received 465 sent 466, DD received 8 sent 8 LS-Req received 2 sent 2, LS-Upd received 8 sent 21 LS-Ack received 14 sent 7, Discarded 3

Common Errors

- The configured neighbor dead time is shorter than the Hello interval.

5.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears and resets an OSPF process.	**clear ip ospf** [*process-id*] **process**

Displaying

Description	Command
Displays the OSPF process configurations.	**show ip ospf** [*process-id*]
Displays the OSPF internal routing table, including routes to ABRs and ASBRs.	**show ip ospf**[*process-id*] **border-routers**
Displays information about the OSPF LSDB.	**show ip ospf** [*process-id area-id*] **database** [{ **asbr-summary** | **external** | **network** | **nssa-external** | **opaque-area** | **opaque-as** | **opaque-link** | **router** | **summary** }][{ **adv-router** *ip-address*| **self-originate** } |*link-state-id*| **brief**][**database-summary** | **max-age** | **detail**]
Displays OSPF-enabled interfaces.	**show ip ospf** [*process-id*] **interface** [*interface-type interface-number* | **brief**]
Displays the OSPF neighbor list.	**show ip ospf** [*process-id*] **neighbor** [**detail**] [*interface-typeinterface-number*] [*neighbor-id*]
Displays the OSPF routing table.	**show ip ospf** [*process-id*] **route**[**count**]
Displays the number of times SPT is computed in the OSPF area.	**show ip ospf** [*process-id*] **spf**
Displays the summarized route of OSPF redistributed routes.	**show ip ospf**[*process-id*] **summary-address**

Description	Command
Displays OSPF virtual links.	**show ip ospf** [*process-id*] **virtual-links** [*ip-address*]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs OSPF events.	**debug ip ospf events** [**abr**|**asbr**|**lsa**|**nssa**|**os**|**restart**| **router**|**slink**| **vlink**]
Debugs OSPF interfaces.	**debug ip ospf ifsm** [**events**|**status**|**timers**]
Debugs OSPF neighbors.	**debug ip ospf nfsm** [**events** | **status** | **timers**]
Debugs the OSPF NSM.	**debug ip ospf nsm** [**interface** | **redistribute** | **route**]
Debugs OSPF LSAs.	**debug ip ospf lsa** [**flooding** | **generate** | **install** | **maxage** | **refresh**]
Debugs OSPF packets.	**debug ip ospf packet** [**dd**|**detail**|**hello**|**ls-ack**|**ls-request**|**ls-update**|**recv**|**send**]
Debugs OSPF routes.	**debug ip ospf route** [**ase** | **ia** | **install** | **spf** | **time**]

6 Configuring OSPFv3

6.1 Overview

Open Shortest Path First (OSPF) is an Interior Gateway Protocol (IGP) that is used within the Autonomous System (AS) to allow routers to obtain a route to a remote network.

OSPF Version 2 (OSPFv2) is applicable to IPv4, and OSPF Version 3 (OSPFv3) is applicable to IPv6. The protocol running mechanism and most configurations are the same.

OSPF has the following characteristics:

- Wide scope of application: OSPF is applicable to a larger-scale network that supports hundreds of routers.
- Fast convergence: Once the network topology changes, notifications can be quickly sent between routers to update routes.
- No self-loop: Only the link status information is synchronized between routers. Each router computes routes independently, and a self-loop will not occur.
- Area division: A large routing domain is divided into multiple small areas to save system resources and network bandwidth and ensure stability and reliability of routes.
- Route classification: Routes are classified into several types to support flexible control.
- Equivalent routes: OSPF supports equivalent routes.
- Authentication: OSPF supports packet authentication to ensure security of protocol interaction.
- Multicast transmission: Protocol packets are sent using the multicast address to avoid interfering with irrelevant entities and save system resources.

In this chapter, the term "router" refers to any network device that supports the routing function. These network devices can be L3 switches, routers, or firewall.

Unless otherwise specified, "OSPF" in the following descriptions refers to OSPFv3.

Protocols and Standards

RFC2740	This document describes the modifications to OSPF to support version 6 of the Internet Protocol (IPv6).
draft-ietf-ospf-ospfv3-graceful-restart	This document describes the OSPFv3 graceful restart. The OSPFv3 graceful restart is identical to OSPFv2 except for the differences described in this document. These differences include the format of the grace Link State Advertisements (LSA) and other considerations.
draft-ietf-ospf-ospfv3-mib-11	This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in IPv6-based internets. In particular, it defines objects for managing the Open Shortest Path First Routing Protocol for IPv6.

6.2 Applications

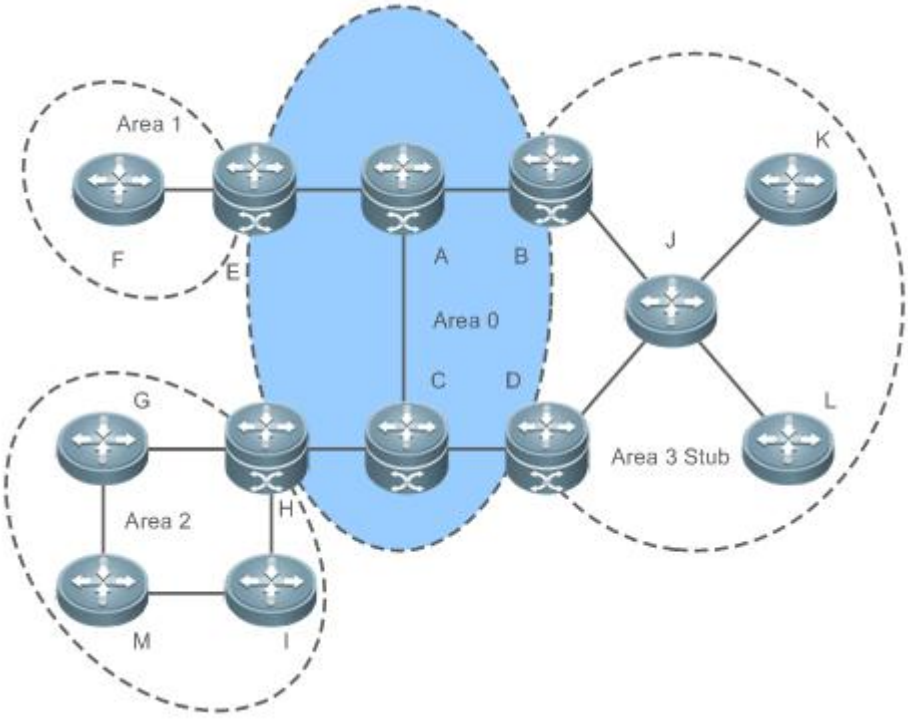
Application	Description
Intra-Domain Interworking	OSPF runs within the AS, which is divided into several areas.
Inter-Domain Interworking	Several ASs are interconnected. OSPF runs within each AS, and BGP runs between ASs.

6.2.1 Intra-Domain Interworking

Scenario

OSPF runs within the AS. If the number of routers exceeds 40, it is recommended that the AS be divided into several areas. Generally, high-end devices featuring reliable performance and fast processing speed are deployed in a backbone area, and low-end or medium-range devices with relatively lower performance can be deployed in a normal area. All normal areas must be connected to the backbone area. It is recommended that a normal area located on the stub be configured as a stub area. As shown in Figure 6- 1, the network is divided into four areas. Communication between these areas must go through the backbone area, that is, area 0.

Figure 6- 1 Division of the OSPF Areas



Remarks	A, B, C, D, E, and H are located in the backbone area, and are backbone routers. Area 3 is configured as a stub area.

Deployment

- OSPF runs on all routers within the AS to implement unicast routing.

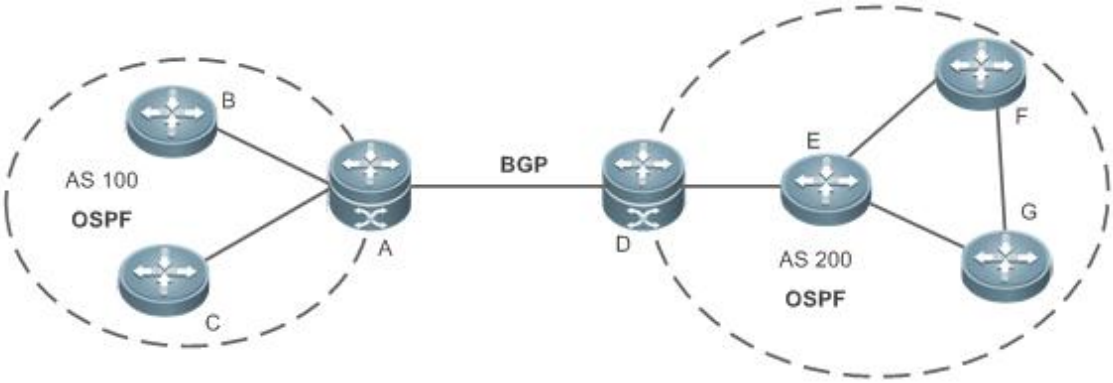
6.2.2 Inter-Domain Interworking

Scenario

Several ASs are interconnected. OSPF runs within each AS, and BGP runs between ASs.Generally, OSPF and BGP learn the routing information from each other.

As shown in Figure 6- 2, unicast routing is implemented within AS 100 and AS 200 using OSPF, and between the two ASs using BGP.

Figure 6- 2 Interworking Between OSPF and BGP



Remarks	OSPF and BGP run concurrently on Router A and Router D.

Deployment

- OSPF runs within AS 100 and AS 200 to implement unicast routing.
- BGP runs between the two ASs to implement unicast routing.

6.3 Features

Basic Concepts

Routing Domain

All routers in an AS must be interconnected and use the same routing protocol. Therefore, an AS is also called a routing domain.
An AS on which OSPF runs is also called OSPF routing domain, or OSPF domain for short.

OSPF Process

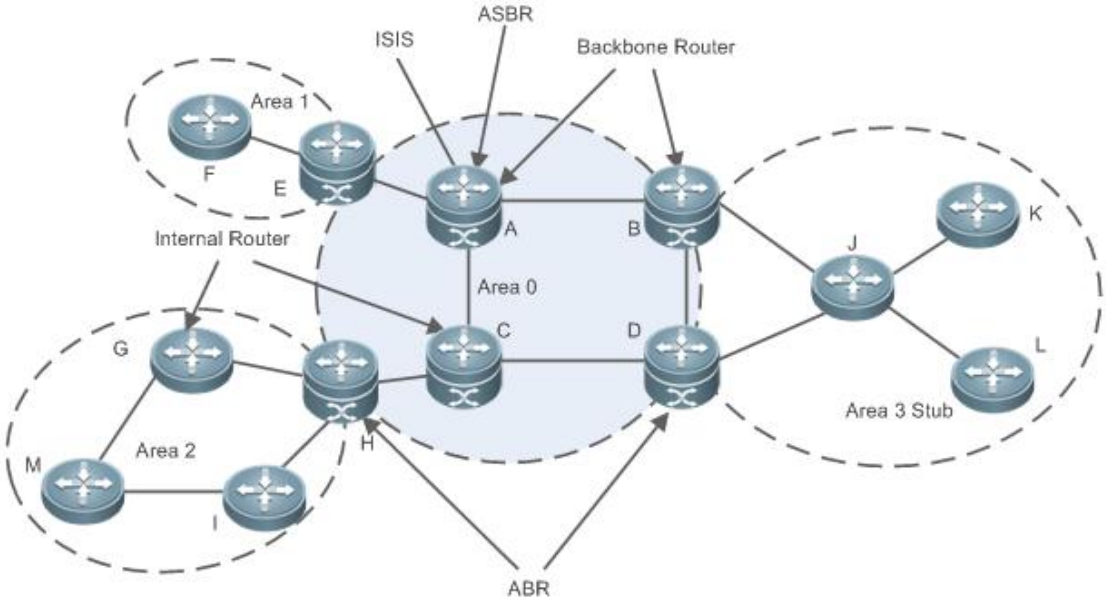
OSPF supports multiple instances, and each instance corresponds to an OSPF process.
One or more OSPF processes can be started on a router. Each OSPF process runs OSPF independently, and the processes are mutually isolated.
An OSPF packet header contains the Instance ID field, and multiple OSPF instances can run concurrently on a single link. The process ID is valid only on the local device.

Router ID

The router ID uniquely identifies a router in an OSPF domain. Router IDs of any two routers cannot be the same.
If multiple OSPF processes exist on a router, each OSPF process uses one router ID. Router IDs of any two OSPF processes cannot be the same.

Area

OSPF supports multiple areas. An OSPF domain is divided into multiple areas to ease the computing pressure of a large-scale network.
An area is a logical group of routers, and each group is identified by an area ID. The border between areas is a router. A router may belong to one area or multiple areas. One network segment (link) can belong to only one area, or each OSPF-enabled interface must belong to a specified area.
Area 0 is the backbone area, and other areas are normal areas. Normal areas must be directly connected to the backbone area.
Figure 6- 3 Division of the OSPF Areas



OSPF Router

The following types of routers are defined in OSPF, and assigned with different responsibilities:

- Internal router

  All interface of an interval router belong to the same OSPF area. As shown in Figure 6- 3, A, C, F, G, I, M, J, K, and L are internal routers.

- Area border router (ABR)

  An ABR is used to connect the backbone area with a normal area. An ABR belongs to two or more areas, and one of the areas must be the backbone area. As shown in Figure 6- 3, B, D, E, and H are ABRs.

- Backbone router

  A backbone router has at least one interface that belongs to the backbone area. All ABRs and all routers in area 0 are backbone routers. As shown in Figure 6- 3, A, B, C, D, E, and H are backbone routers.

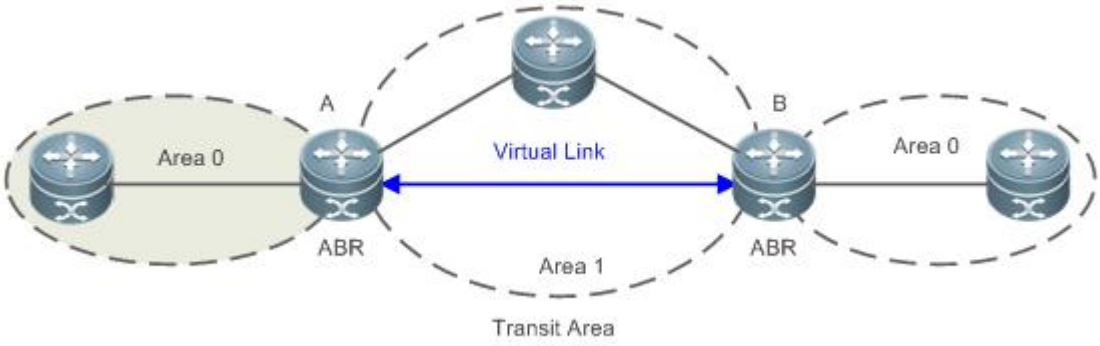
- AS boundary router (ASBR)

  An ASBR is used to exchange routing information with other ASs. An ASBR is not necessarily located on the border of an AS. It may be a router inside an area, or an ABR. As shown in Figure 6- 3, A is an ASBR.

Virtual Link

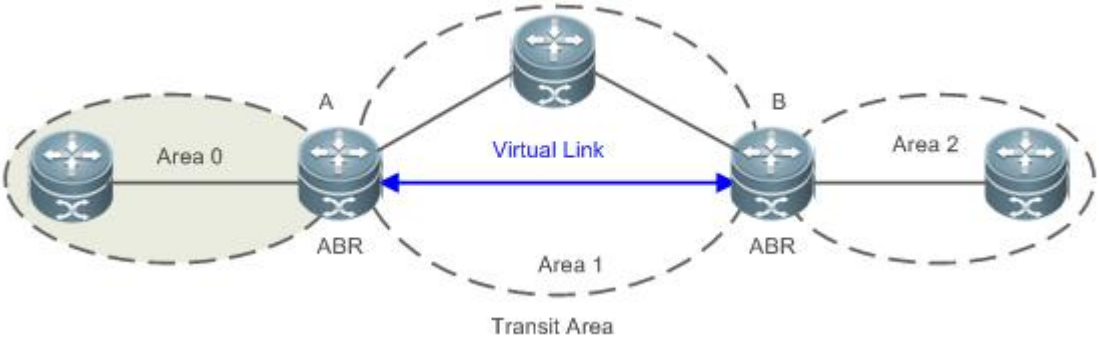
OSPF supports virtual links. A virtual link is a logical link that belongs to the backbone area. It is used to resolve the problems such as a discontinuous backbone area or a failure to directly connect a normal area to the backbone area on the physical network. A virtual link supports traversal of only one normal area, and this area is called transit area. Routers on both ends of a virtual link are ABRs.

Figure 6- 4 Discontinuous Backbone Area on the Physical Network



As shown in Figure 6- 4, a virtual link is set up between A and B to connect two separated parts of Area 0. Area 1 is a transit area, and A and B are ABRs of Area 1.

Figure 6- 5Failure to Directly Connect a Normal Area to the Backbone Area on the Physical Network



As shown in Figure 6- 5, a virtual link is set up between A and B to extend Area 0 to B so that Area 0 can be directly connected to Area 2 on B. Area 1 is a transit area, A is an ABR of Area 1, and B is an ABR of Area 0 and Area 2.

↘ LSA

OSPF describes the routing information by means of Link State Advertisement (LSA).

LSA Type	Description
Router-LSA(Type1)	This LSA is originated by every router. It describes the link state and cost of the router, and is advertised only within the area where the originating router is located.
Network-LSA(Type2)	This LSA is originated by a designated router (DR). It describes the state of the current link, and is advertised only within the area where the DR is located.
Inter-Area-Prefix-LSA(Type3)	This LSA is originated by an ABR. It describes a route to another area, and is advertised to areas except totally stub areas or Not-So-Stubby Area (NSSA) areas.
Inter-Area-Router-LSA(Type4)	This LSA is originated by an ABR. It describes a route to an ASBR, and is advertised to areas except areas where the ASBR is located.
AS-external-LSA(Type5)	This LSA is originated by an ABR. It describes a route to a destination outside the AS, and is advertised to all areas except the stub and NSSA areas.
NSSA LSA(Type7)	This LSA is originated by an ABR. It describes a route to a destination outside the AS, and is advertised only within the NASSA areas.
Link-LSA(Type8)	This LSA is originated by every router. It describes the link-local address and IPv6 prefix address of each link, and provides the link option that will be set in the Network-LSA. It advertised only on the current link.
Intra-Area-Prefix-LSA(Type9)	Every router or DR generates one or more Intra-Area-Prefix-LSAs, which are advertised in the area to which the router or DR belongs.

LSA Type	Description
	● The Intra-Area-Prefix-LSA generated by a router describes the IPv6 prefix address associated with the Route-LSA. ● The Intra-Area-Prefix-LSA generated by a DR describes the IPv6 prefix address associated with the Network-LSA.

Stub areas, NSSA areas, totally stub areas, and totally NSSA areas are special forms of normal areas and help reduce the load of routers and enhance reliability of OSPF routes.

OSPF Packet

The following table lists the protocol packets used by OSPF. These OSPF packets are encapsulated in IP packets and transmitted in multicast or unicast mode.

Packet Type	Description
Hello	Hello packets are sent periodically to discover and maintain OSPF neighbor relationships.
Database Description (DD)	DD packets carry brief information about the local Link-State Database (LSDB) and are used to synchronize the LSDBs between OSPF neighbors.
Link State Request (LSR)	LSR packets are used to request the required LSAs from neighbors. LSR packets are sent only after DD packets are exchanged successfully between OSPF neighbors.
Link State Update (LSU)	LSU packets are used to send the required LSAs to peers.
Link State Acknowledgment (LSAck)	LSAck packets are used to acknowledge the received LSAs.

Overview

Feature	Description
Link-State Routing Protocols	Run OSPF on the router to obtain routes to different destinations on the network.
OSPF Route Management	Properly plan or optimize OSPF routes through manual configuration to implement management of OSPF routes.
Enhanced Security and Reliability	Use functions such as authentication and BFD correlation to enhance security, stability, and reliability of OSPF.
Network Management Functions	Use functions such as the MIB and Syslog to facilitate OSPF management.

6.3.1 Link-State Routing Protocols

OSPF is a type of link-state routing protocols. Its working process is as follows:

- Neighbor discovery → Bidirectional communication
  An OSPF neighbor relationship is set up between adjacent routers, and bidirectional communication is maintained.
- Database synchronization → Full adjacency
  A router uses LSAs to advertise all its link states. LSAs are exchanged between neighbors and the link state database (LSDB) is synchronized to achieve full adjacency.
- Shortest Path Tree (SPT) computation → Formation of a routing table
  The router computes the shortest path to each destination network based on the LSDB and forms an OSPF routing table.

Working Principle

Neighbor Discovery → Bidirectional Communication

Routers send Hello packets through all OSPF-enabled interfaces (or virtual links). If Hello packets can be exchanged between two routers, and parameters carried in the Hello packets can be successfully negotiated, the two routers become neighbors. Routers that are mutually neighbors find their own router IDs from Hello packets sent from neighbors, and bidirectional communication is set up.

A Hello packet includes, but is not limited to, the following information:

- Router ID of the originating router
- Area ID of the originating router interface (or virtual link)
- Instance ID of the originating router interface (or virtual link)
- Interface ID of the originating router interface (or virtual link)
- Priority of the originating router interface (used for DR/BDR election)
- Hello interval of the originating router interface (or virtual link)
- Neighbor dead interval of the originating router interface (or virtual link)
- IP addresses of the DR and Backup Designated Router (BDR)
- Router ID of the neighbor of the originating router

Database Synchronization → Full Adjacency

After bidirectional communication is set up between neighbor routers, the DD, LSR, LSU, and LSAck packets are used to exchange LSAs and set up the adjacency. The brief process is as follows:

- A router generates an LSA to describe all link states on the router.
- The LSA is exchanged between neighbors. When a router receives the LSA from its neighbor, it copies the LSA and saves the copy in the local LSDB, and then advertises the LSA to other neighbors.
- When the router and its neighbors obtain the same LSDB, full adjacency is achieved.

OSPF will be very quiet without changes in link costs or network addition or deletion. If any change takes place, the changed link states are advertised to quickly synchronize the LSDB.

SPT Computation → Formation of a Routing Table

After the complete LSDB is obtained from the router, the Dijkstra algorithm is run to generate an SPT from the local router to each destination network. The SPT records the destination networks, next-hop addresses, and costs. OSPF generates a routing table based on the SPT.

If changes in link costs or network addition or deletion take place, the LSDB will be updated. The router again runs the Dijkstra algorithm, generates a new SPT, and updates the routing table.

The Dijkstra algorithm is used to find a shortest path from a vertex to other vertices in a weighted directed graph.

OSPF Network Types

A router does not necessarily need to exchange LSAs with every neighbor and set up an adjacency with every neighbor. To improve efficiency, OSPF classifies networks that use various link layer protocols into five types so that LSAs are exchanged in different ways to set up an adjacency:

- Broadcast

  Neighbors are discovered, and the DR and BDR are elected.

The DR (or BDR) exchanges LSAs with all other routers to set up an adjacency. Except the DR and BDR, all other routers do not exchange LSAs with each other, and the adjacency is not set up.

Ethernet and fiber distributed data interface (FDDI) belong to the broadcast network type by default.

- Non-broadcast multiple access (NBMA)

Neighbors are manually configured, and the DR and BDR are elected.

The DR (or BDR) exchanges LSAs with all other routers to set up an adjacency. Except the DR and BDR, all other routers do not exchange LSAs with each other, and the adjacency is not set up.

X.25, frame relay, and ATM belong to NBMA networks by default.

- Point-to-point (P2P)

Neighbors are automatically discovered, and the DR or BDR is not elected.

LSAs are exchanged between routers at both ends of the link, and the adjacency is set up.

PPP, HDLC, and LAPB belong to the P2P network type by default.

- Point-to-multipoint(P2MP)

Neighbors are automatically discovered, and the DR or BDR is not elected.

LSAs are exchanged between any two routers, and the adjacency is set up.

Networks without any link layer protocol belong to the P2MP network type by default.

- P2MP broadcast

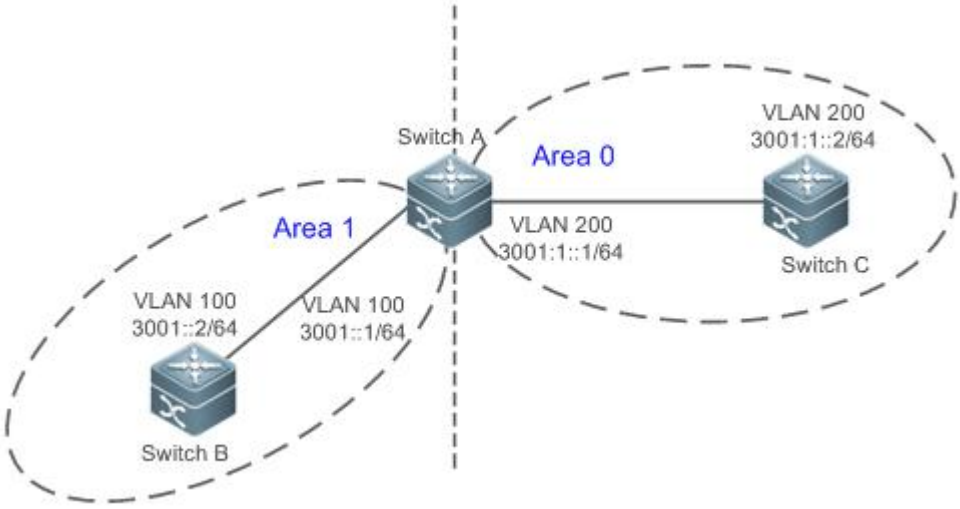
Neighbors are manually configured, and the DR or BDR is not elected.

LSAs are exchanged between any two routers, and the adjacency is set up.

Networks without any link layer protocol belong to the P2MP network type by default.

OSPF Route Types

Figure 6- 6



Display the OSPF routes (marked in red) in the routing table of Router C.

```
C#show ipv6 route ospf
```

```
IPv6 routing table name is Default(0) global scope - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
        O - OSPF intra area, OI - OSPF inter area,   OE1 - OSPF external type 1, OE2 - OSPF external type 2
        ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
        [*] - NOT in hardware forwarding table

L       ::1/128    via Loopback, local host
OI      3001::/64    [110/2] via FE80::21A:A9FF:FE15:4CB9, VLAN 200
C       3001:1::/64    via VLAN 200, directly connected
L       3001:1::2/128    via VLAN 200, local host
L       FE80::/10    via ::1, Null0
C       FE80::/64    via VLAN 200, directly connected
L       FE80::21A:A9FF:FE01:FB1F/128    via VLAN 200, local host
```

A mark is displayed in front of each OSPF route to indicate the type of the route. There are six types of OSPF routes:

- O: Intra-area route

  This type of route describes how to arrive at a destination network in the local area. The cost of this type of route is equal to the cost of the route from the local router to the destination network.

- OI: Inter-area route

  This type of route describes how to arrive at a destination network in another area. The cost of this type of route is equal to the cost of the route from the local router to the destination network.

- OE1: Type 1 external route

  This type of route describes how to arrive at a destination network outside the AS. The cost of this type of route is equal to the cost of the route from the local router to the ASBR plus the cost of the route from the ASBR to the destination network. This type of route does not exist on routers in the stub or NSSA area.

- OE2: Type 2 external route

  This type of route describes how to arrive at a destination network outside the AS. The cost of this type of route is equal to the cost of the route from the ASBR to the destination network. This type of route does not exist on routers in the stub or NSSA area.

- ON1: Type 1 external route of the NSSA area

  This type of route describes how to arrive at a destination network outside the AS through the ASBR in the NSSA area. The cost of this type of route is equal to the cost of the route from the local router to the ASBR plus the cost of the route from the ASBR to the destination network. This type of route exists only on routers in the NSSA area.

- ON2: Type 2 external route of the NSSA area

  This type of route describes how to arrive at a destination network outside the AS through the ASBR in the NSSA area. The cost of this type of route is equal to the cost of the route from the ASBR to the destination network. This type of route exists only on routers in the NSSA area.

Reliability of OE2 and ON2 routes is poor. OSPF believes that the cost of the route from the ASBR to a destination outside an AS is far greater than the cost of the route to the ASBR within the AS. Therefore, when the route cost is computed, only the cost of the route from the ASBR to a destination outside an AS is considered.

Related Configuration

Enabling OSPF

OSPF is disabled by default.

Run the **ipv6 router ospf** 1 command to create an OSPF process on the router.

Run the **ipv6 ospfarea** command to enable OSPF on an interface and specify the area ID.

Run the **area virtual-link** command to create a virtual link on the router. The virtual link can be treated as a logical interface.

Router ID

By default, the OSPF process elects the largest IPv4 address among the IPv4 addresses of all the loopback interfaces as the router ID. If the loopback interfaces configured with IPv4 addresses are not available, the OSPF process elects the largest IPv4 address among the IPv4 addresses of all the physical ports as the router ID.

Alternatively, you can run the **router-id** command to manually specify the router ID.

Protocol Control Parameters

Run the **ipv6 ospf hello-interval** command to modify the Hello interval on the interface. The default value is 10s (or 30s for NBMA networks).

Run the **ipv6 ospf dead-interval** command to modify the neighbor dead interval on the interface. The default value is four times the Hello interval.

Use the **poll-interval** parameter in the **ipv6 ospf neighbor** command to modify the neighbor polling interval on the NBMA interface. The default value is 120s.

Run the **ipv6 ospf transmit-delay** command to modify the LSU packet transmission delay on the interface. The default value is 1s.

Run the **ipv6 ospf retransmit-interval** command to modify the LSU packet retransmission interval on the interface. The default value is 5s.

Use the **hello-interval** parameter in the **area virtual-link** command to modify the Hello interval on the virtual link. The default value is 10s.

Use the **dead-interval** parameter in the **area virtual-link** command to modify the neighbor dead interval on the virtual link. The default value is four times the Hello interval.

Use the **transmit-delay** parameter in the **area virtual-link** command to modify the LSU packet transmission delay on the virtual link. The default value is 1s.

Use the **retransmit-interval** parameter in the **area virtual-link** command to modify the LSU packet retransmission interval on the virtual link. The default value is 5s.

Run the **timers throttle lsa all** command to modify parameters of the exponential backoff algorithm that generates LSAs. The default values of these parameters are 0 ms, 5000 ms, and 5000 ms.

Run the **timers pacing lsa-group** command to modify the LSA group update interval. The default value is 30s.

Run the **timers pacing lsa-transmit** command to modify the LS-UPD packet sending interval and the number of sent LS-UPD packets. The default values are 40 ms and 1.

Run the **timers lsa arrival** command to modify the delay after which the same LSA is received. The default value is 1000 ms.

Run the **timers throttle spf** command to modify the SPT computation delay, minimum interval between two SPT computations, and maximum interval between two SPT computations. The default values are 1000 ms, 5000 ms, and 10000 ms.

OSPF Network Types

By default, Ethernet and FDDI belong to the broadcast type, X.25, frame relay, and ATM belong to the NBMA type, and PPP, HDLC, and LAPB belong to the P2P type.

Run the **ipv6 ospf network** command to manually specify the network type of an interface.

Run the **ipv6 ospf neighbor** command to manually specify a neighbor. For the NBMA and P2MP non-broadcast types, you must manually specify neighbors.

Run the **ipv6 ospf priority** command to adjust the priorities of interfaces, which are used for DR/BDR election. The DR/BDR election is required for the broadcast and NBMA types. The router with the highest priority wins in the election, and the router with the priority of 0 does not participate in the election. The default value is 1.

6.3.2 OSPF Route Management

Properly plan or optimize OSPF routes through manual configuration to implement management of OSPF routes.

Working Principle

(Totally) Stub Area and (Totally) NSSA Area

The (totally) stub and (totally) NSSA areas help reduce the protocol interaction load and the size of the routing table.

- If an appropriate area is configured as a (totally) stub or NSSA area, advertisement of a large number of Type 5 and Type 3 LSAs can be avoided within the area.

Area	Type 1 and Type 2 LSAs	Type 3 LSA	Type 4 LSA	Type 5 LSA	Type 7 LSA
Non (totally) stub area and NSSA area	Allowed	Allowed	Allowed	Allowed	Not allowed
Stub area	Allowed	Allowed (containing one default route)	Not allowed	Not allowed	Not allowed
Totally stub area	Allowed	Only one default route is allowed.	Not allowed	Not allowed	Not allowed
NSSA area	Allowed	Allowed (containing one default route)	Allowed	Not allowed	Allowed
Totally NSSA area	Allowed	Only one default route is allowed.	Allowed	Not allowed	Allowed

The ABR uses Type 3 LSAs to advertise a default route to the (totally) stub or NSSA area.

The ABR converts Type 7 LSAs in the totally NSSA area to Type 5 LSAs, and advertise Type 5 LSAs to the backbone area.

- If an area is appropriately configured as a (totally) stub area or an NSSA area, a large number of OE1, OE2, and OI routes will not be added to the routing table of a router in the area.

Area	Routes Available in the Routing Table of a Router Inside the Area
Non (totally) stub area and NSSA area	O: a route to a destination network in the local area OI: a route to a destination network in another area OE1 or OE2: a route or default route to a destination network segment outside the AS (via any ASBR in the AS)
Stub area	O: a route to a destination network in the local area OI: a route or a default route to a destination network in another area

Area	Routes Available in the Routing Table of a Router Inside the Area
Totally stub area	O: a route to a destination network in the local area OI: a default route
NSSA area	O: a route to a destination network in the local area OI: a route or a default route to a destination network in another area ON1 or ON2: a route or default route to a destination network segment outside the AS (via an ASBR in the local area)
Totally NSSA area	O: a route to a destination network in the local area OI: a default route ON1 or ON2: a route or default route to a destination network segment outside the AS (via an ASBR in the local area)

Route Redistribution

Route redistribution refers to the process of introducing routes of other routing protocols, routes of other OSPF processes, static routes, and direct routes that exist on the device to an OSPF process so that these routes can be advertised to neighbors using Type 5 and Type 7 LSAs. A default route cannot be introduced during route redistribution.

Route redistribution is often used for interworking between ASs. You can configure route redistribution on an ASBR to advertise routes outside an AS to the interior of the AS, or routes inside an AS to the exterior of the AS.

Default Route Introduction

By configuring a command on an ASBR, you can introduce a default route to an OSPF process so that the route can be advertised to neighbors using Type 5 and Type 7 LSAs.

Default route introduction is often used for interworking between ASs. One default route is used to replace all the routes outside an AS.

Route Summarization

Route summarization is a process of summarizing routing information with the same prefix into one route, and advertising the summarized route (replacing a large number of individual routes) to neighbors. Route summarization helps reduce the protocol interaction load and the size of the routing table.

By default, the ABR advertises inter-area routing information by using Type3 LSAs within a network segment, and advertises redistributed routing information by using Type 5 and Type 7 LSAs.If continuous network segments exist, it is recommended that you configure route summarization.

Route Filtering

OSPF supports route filtering to ensure security and facilitate control when the routing information is being learned, exchanged, or used.

Using configuration commands, you can configure route filtering for the following items:

- Interface: The interface is prevented from sending routing information (any LSAs) or exchanging routing information (any LSAs) with neighbors.
- Routing information outside an AS: Only the routing information that meets the filtering conditions can be redistributed to the OSPF process (Type 5 and Type 7 LSAs).
- LSAs received by a router: In the OSPF routing table, only the routes that are computed based on the LSAs meeting the filtering conditions can be advertised.

Route Cost

If redundancy links or devices exist on the network, multiple paths may exist from the local device to the destination network. OSPF selects the path with the minimum total cost to form an OSPF route. The total cost of a path is equal to the sum of the costs of individual links along the path.The total cost of a path can be minimized by modifying the costs of individual links along the path. In this way, OSPF selects this path to form a route.

Using configuration commands, you can modify the following link costs:

- Cost from an interface to a directly connected network segment and cost from the interface to a neighbor
- Cost from an ABR to the default network segment
- Cost from an ASBR to an external network segment and cost from the ASBR to the default network segment

Both the cost and the metric indicate the cost and are not differentiated from each other.

OSPF Administrative Distance

The administrative distance (AD) evaluates reliability of a route, and the value is an integer ranging from 0 to 255. A smaller AD value indicates that the route is more trustworthy. If multiples exist to the same destination, the route preferentially selects a route with a smaller AD value. The route with a greater AD value becomes a floating route, that is, a standby route of the optimum route.
By default, the route coming from one source corresponds to an AD value. The AD value is a local concept. Modifying the AD value affects route selection only on the current router.

Route Source	Directly-connected network	Static route	EBGP Route	OSPF Route	IS-IS Route	RIP Route	IBGP Route	Unreachable Route
Default AD	0	1	20	110	115	120	200	255

Related Configuration

Stub Area and NSSA Area

By default, no stub or NSSA area is configured.

Run the **area stub** command to configure a specified area as a stub area.

Run the **area nssa** command to configure a specified area as an NSSA area.

A backbone area cannot be configured as a stub or an NSSA area.

A transit area (with virtual links going through) cannot be configured as a stub or an NSSA area.

An area containing an ASBR cannot be configured as a stub area.

Route Redistribution and Default Route Introduction

By default, routes are not redistributed and the default route is not introduced.

Run the **redistribute** command to configure route redistribution.

Run the **default-information originate** command to introduce a default route.

After configuring route redistribution and default route introduction, the router automatically becomes an ASBR.

Route Summarization

By default, routes are not summarized. If route summarization is configured, a discard route will be automatically added.

Run the **area range** command to summarize routes (Type 3 LSA) distributed between areas on the ABR.

Run the **summary-prefix** command to summarize redistributed routes (Type 5 and Type 7 LSAs) on the ASBR.

Route Filtering

By default, routes are not filtered.

Run the **passive-interface** command to configure a passive interface. Routing information (any LSAs) cannot be exchanged on a passive interface.

Use the **route-map** parameter in the **redistribute** command, or use the **distribute-list out** command to filter the external routing information of the AS on the ASBR. Only the routing information that meets the filtering conditions can be redistributed to the OSPF process (Type 5 LSAs).

Run the **distribute-list in** command to filter LSAs received by the router. In the OSPF routing table, only the routes that are computed based on the LSAs meeting the filtering conditions can be advertised.

Route Cost

- Cost from the interface to the directly-connected network segment (cost on the interface)
- The default value is the auto cost. Auto cost = Reference bandwidth/Interface bandwidth
- Run the **auto-cost reference-bandwidth** command to set the reference bandwidth of the auto cost. The default value is 100 Mbps.
- Run the **ipv6 ospf cost** command to manually set the cost of the interface. The configuration priority of this item is higher than that of the auto cost.
- Cost from the interface to a specified neighbor (that is, cost from the local device to a specified neighbor)
- The default value is the auto cost.
- Use the **cost** parameter in the **ipv6 ospf neighbor** command to modify the cost from the interface to a specified neighbor. The configuration priority of this item is higher than that of the cost of the interface.
- This configuration item is applicable only to P2MP-type interfaces.
- Cost from the ABR to the default network segment (that is, the cost of the default route that is automatically advertised by the ABR to the stub or NSSA areas)
- The default value is 1.
- Run the **area default-cost** command to modify the cost of the default route that the ABR automatically advertise to the stub areas.
- Cost from the ASBR to an external network segment (that is, the metric of an external route)
- By default, the metric of a redistributed BGP route is 1, the metric of other types of redistributed routes is 20, and the route type is Type 2 External.
- Run the **default-metric** command to modify the default metric of the external route.
- Use the **metric**,**metric-type**, and **route-map** parameters in the **redistribute** command to modify the metric and route type of the external route.
- Cost from the ASBR to the default network segment (that is, the metric of the default route that is manually introduced)
- By default, the metric is 1, and the route type is Type 2 External.

- Use the **metric**,**metric-type**, and **route-map** parameters in the **default-information originate** command to modify the metric and route type of the default route that is manually introduced.

OSPF Administrative Distance

By default, the OSPF AD is 110.

Run the **distance** command to set the AD of an OSPF route.

6.3.3 Enhanced Security and Reliability

Use functions such as authentication and BFD correlation to enhance security, stability, and reliability of OSPF.

Working Principle

Authentication

OSPFv3 uses the authentication mechanism, that is, IP authentication header (AH) and IP Encapsulating Security Payload (ESP), provided by IPv6 to prevent unauthorized routers that access the network and hosts that forge OSPF packets to participate in OSPF routing. OSPF packets received on the OSPF interface (or at both ends of a virtual link) are authenticated. If authentication fails, the packets are discarded and the adjacency cannot be set up.

Enabling authentication can avoid learning unauthenticated or invalid routes, thus preventing advertising valid routes to unauthenticated devices. In the broadcast-type network, authentication also prevents unauthenticated devices from becoming designated devices, ensuring stability of the routing system and protecting the routing system against intrusions.

MTU Verification

On receiving a DD packet, OSPF checks whether the MTU of the neighbor interface is the same as the MTU of the local interface. If the MTU of the interface specified in the received DD packet is greater than the MTU of the interface that receives the packet, the adjacency cannot be set up. Disabling MTU verification can avoid this problem.

Two-Way Maintenance

OSPF routers periodically send Hello packets to each other to maintain the adjacency. On a large network, a lot of packets may be sent or received, occupying too much CPU and memory. As a result, some packets are delayed or discarded. If the processing time of Hello packets exceeds the dead interval, the adjacency will be destroyed.

If the two-way maintenance function is enabled, in addition to the Hello packets, the DD, LSU, LSR, and LSAck packets can also be used to maintain the bidirectional communication between neighbors, which makes the adjacency more stable.

Concurrent neighbor Interaction Restriction

When a router simultaneously exchanges data with multiple neighbors, its performance may be affected. If the maximum number of neighbors that concurrently initiate or accept interaction with the OSPF process, the router can interact with neighbors by batches, which ensures data forwarding and other key services.

Compatibility with Type-9 LSA with IPv6 Prefix

By default, type-9 LSA can not have IPv6 prefix.

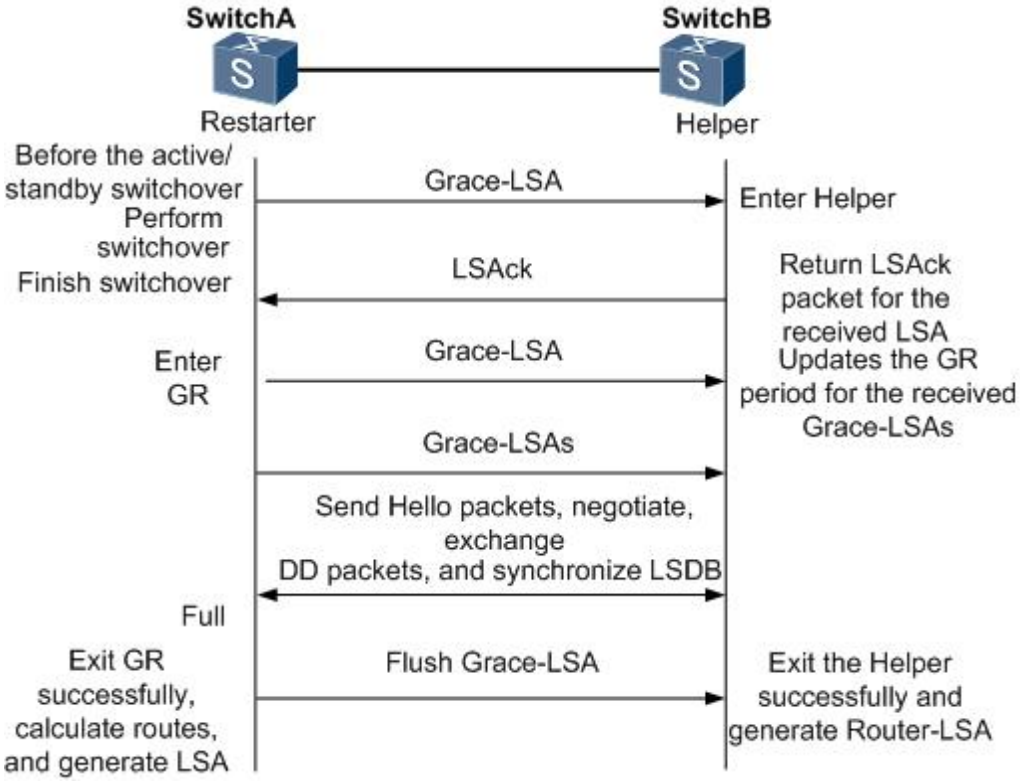
Run the **ipv6 router ospf compatible lsa type-9** command, the type-9 LSA generated by device will have Ipv6 prefix.

GR

The control and forwarding separated technology is widely used among routers. On a relatively stable network topology, when a GR-enabled router is restarted on the control plane, data forwarding can continue on the forwarding plane. In addition, actions (such as adjacency re-forming and route computation) performed on the control plane do not affect functions of the forwarding plane. In this way, service interruption caused by route flapping can be avoided, thus enhancing reliability of the entire network.

Currently, the GR function is used only during active/standby switchover and system upgrade.

Figure 6- 7Normal OSPF GR Process



- The GR process requires collaboration between the restarter and the helper. The restarter is the router where GR occurs. The helper is a neighbor of the restarter.
- When entering or exiting the GR process, the restarter sends a Grace-LSA to the neighbor, notifying the neighbor to enter or exit the helper state.
- When the adjacency between the restarter and the helper reaches the Full state, the router can exit the GR process successfully.

Fast Hello and BFD Correlation

After a link fault occurs, it takes a period of time (about 40s) before OSPF can sense the death of the neighbor. Then, OSPF advertises the information and re-computes the SPT. During this period, traffic is interrupted.

- After the fast Hello function is enabled (that is, the neighbor dead interval is set to 1s), OSPF can sense the death of a neighbor within 1s once a link is faulty. This greatly accelerates route convergence and prevents traffic interruption.
- BFD is used to test connectivity between devices. A link fault can be detected in as short as 150 ms. After OSPF is correlated with BFD, OSPF can sense the death of a neighbor in as short as 150 ms once a link is faulty. This greatly accelerates route convergence and prevents traffic interruption.

Related Configuration

OSPF Packet Authentication

By default, authentication is disabled.

- Run the **area authentication** command to enable authentication in the entire area so that the authentication function takes effect on all interfaces in this area. If authentication is enabled in area 0, the function also takes effect on the virtual link.
- Run the **area encryption** command to enable encryption and authentication in the entire area so that the encryption**and** authentication functions take effect on all interfaces in this area. If encryptionand authentication are enabled in area 0, the functions also take effect on the virtual link.
- Run the **ipv6 ospf authentication** command to enable authentication on an interface. This configuration takes precedence over the area-based configuration.
- Run the **ipv6 ospf encryption** command to enable encryptionand authentication on an interface. This configuration takes precedence over the area-based configuration.
- Use the **authentication** parameter in the **area virtual-link** command to enable authentication at both ends of a virtual link. This configuration takes precedence over the area-based configuration.
- Use the **encryption** parameter in the **area virtual-link** command to enable encryptionand authentication at both ends of a virtual link. This configuration takes precedence over the area-based configuration.

MTU Verification

By default, MTU verification is disabled.

Run the **ipv6 ospf mtu-ignore** command to disable MTU verification on an interface.

Two-Way Maintenance

By default, bidirectional maintenance is enabled.

Run the **two-way-maintain** command to enable two-way maintenance.

Concurrent neighbor Interaction Restriction

Run the **max-concurrent-dd** command to modify the maximum number of neighbors that are concurrently interacting with the current OSPF process. The default value is 5.

Run the **ipv6 router ospf max-concurrent-dd** command to modify the maximum number of neighbors that are concurrently interacting with all OSPF processes on the router. The default value is 10.

GR

By default, the restarter function is disabled, and the helper function is enabled.

Run the **graceful-restart** command to configure the restarter function.

Run the **graceful-restart helper** command to configure the helper function.

Fast Hello

By default, the neighbor dead interval on the interface is 40s.

Run the **ipv6 ospf dead-interval minimal hello-multiplier** command to enable the Fast Hello function on an interface, that is, the neighbor dead interval is 1s.

Correlating OSPF with BFD

By default, OSPF is not correlated with BFD.

Run the **bfd interval min_rx multiplier** command to set the BFD parameters.

Run the **bfd all-interfaces** command to correlate OSPF with BFD on all interfaces.

Run the **ipv6 ospf bfd** command to correlate OSPF with BFD on the current interface.

6.3.4 Network Management Functions

Use functions such as the MIB and Syslog to facilitate OSPF management.

Working Principle

- **MIB**

MIB is the device status information set maintained by a device. You can use the management program to view and set the MIB node.

Multiple OSPF processes can be simultaneously started on a router, but the OSPF MIB can be bound with only one OSPF process.

- **Trap**

A trap message is a notification generated when the system detects a fault. This message contains the related fault information.

If the trap function is enabled, the router can proactively send the trap messages to the network management device.

- **Syslog**

The Syslog records the operations (such as command configuration) performed by users on routers and specific events (such as network connection failures).

If the syslog is allowed to record the adjacency changes, the network administrator can view the logs to learn the entire process that the OSPF adjacency is set up and maintained.

Related Configuration

- **MIB**

By default, the MIB is bound with the OSPF process with the smallest process ID.

Run the **enable mib-binding** command to bind the MIB with the current OSPF process.

- **Trap**

By default, all traps functions are disabled, and the device is not allowed to send OSPF traps.

Run the **snmp-server enable traps ospf** command to allow the device to send OSPF traps.

Run the **enable traps** command to enable a specified trap function for an OSPF process.

- **Syslog**

By default, the Syslog is allowed to record the adjacency changes.

Run the **log-adj-changes** command to allow the Syslog to record the adjacency changes.

6.4 Configuration

Configuration	Description and Command
Configuring OSPF Basic	(Mandatory)It is used to build an OSPF routing domain.

Configuration	Description and Command	
Functions	**ipv6routerospf**	Creates an OSPF process.
	router-id	Configures a router ID.
	ipv6 ospfarea	Enables OSPF on an interface and specifies an area ID.
	area virtual-link	Creates a virtual link.
Setting the Network Type	(Optional) The configurations are mandatory if the physical network is the X.25, frame relay, or ATM network.	
	ipv6 ospf network	Defines the network type.
	ipv6 ospf neighbor	Specifies a neighbor.
	ipv6 ospf priority	Configures the DR priority.
Configuring Route Redistribution and Default Route	(Optional) The configurations are recommended if the OSPF routing domain is connected with an external network.	
	redistribute	Configures route redistribution.
	default-information originate	Introduces a default route.
Configuring the Stub Area and NSSA Area	(Optional) It is used to reduce interaction of routing information and the size of routing table, and enhance stability of routes.	
	area stub	Configures a stub area.
	area nssa	Configures an NSSA area.
Configuring Route Summarization	(Optional) It is used to reduce interaction of routing information and the size of routing table, and enhance stability of routes.	
	area range	Summarizes routes that are advertised between areas.
	summary-prefix	Summarizes routes that are introduced through redistribution.
Configuring Route Filtering	(Optional) It is used to manually control interaction of routing information and filter available OSPF routes.	
	passive-interface	Configures a passive interface.
	distribute-list out	Filters routes that are introduced through redistribution.
	distribute-listin	Filters received LSAs.
Modifying the Route Cost and AD	(Optional) It is used to manually control the shortest route computed by OSPF and determine whether to select an OSPF route preferentially.	
	auto-cost reference-bandwidth	Modifies the reference bandwidth of the auto cost.
	ipv6 ospf cost	Modifies the cost in the outbound direction of an interface.
	areadefault-cost	Modifies the cost of the default route in a stub or an NSSA area.
	default-metric	Modifies the default metric of a redistributed route.
	distance	Modifies the OSPF AD.

Configuration	Description and Command	
Enabling Authentication	(Optional) It is used to prevent routers that illegally access the network and hosts that forge OSPF packets from participating in the OSPF protocol process.	
	area authentication	Enables authentication and sets the authentication mode in an area.
	area encryption	Enables encryption and authentication and sets the authentication mode in an area.
	ipv6 ospf authentication	Enables authentication and sets the authentication mode on an interface.
	ipv6 ospf encryption	Enables encryption and authentication and sets the authentication mode on an interface.
Modifying the Maximum Number of Concurrent Neighbors	(Optional) It is used to prevent the problem of performance deterioration caused by over-consumption of the CPU.	
	max-concurrent-dd	Modifies the maximum number of con current neighbors on the current OSPF process.
	ipv6 router ospf max-concurrent-dd	Modifies the maximum number of con current neighbors on all OSPF processes.
Disabling MTU Verification	(Optional) It is used to prevent the problem that the adjacency cannot be set up due to MTU inconsistency on the neighbor interface.	
	ipv6 ospf mtu-ignore	Disables MTU verification on an interface.
Enabling Two-Way Maintenance	(Optional) It is used to prevent termination of the adjacency due to the delay or loss of Hello packets.	
	two-way-maintain	Enables two-way maintenance.
Enabling GR	(Optional) It is used to retain OSPF routing forwarding during restart or active/standby switchover of the OSPF processes to prevent traffic interruption.	
	graceful-restart	Enables the restarter function.
	graceful-restart helper	Enables the helper function.
Enabling Fast Hello	(Optional) It is used to quickly discover the death of a neighbor to prevent traffic interruption when a link is faulty.	
	ipv6 ospf dead-intervalminimal hello-multiplier	Enabling the Fast Hello function on an interface.
Configuring Network Management Functions	(Optional) The configurations enable users to use the SNMP network management software to manage OSPF.	
	enable mib-binding	Bind MIB to the OSPF process.
	enable traps	Enables the trap function of the OSPF process.
	log-adj-changes	Allows the syslogs to record the changes in adjacency status.
Modifying Protocol Control Parameters	(Optional) You are advised not to modify protocol control parameters unless necessary.	
	ipv6 ospf hello-interval	Modifies the Hello interval on an interface.
	ipv6 ospf dead-interval	Modifies the neighbor death interval on an interface.

Configuration	Description and Command	
	ipv6 ospf transmit-delay	Modifies the LSU packet transmission delay on an interface.
	ipv6 ospf retransmit-interval	Modifies the LSU packet retransmission interval on an interface.
	timers throttle lsa all	Modifies parameters of the exponential backoff algorithm that generates LSAs.
	timerspacinglsa-group	Modifies the LSA group update interval.
	timers pacing lsa-transmit	Modifies the LS-UPD packet sending interval.
	timers lsa arrival	Modifies the delay after which the same LSA is received.
	timers throttlespf	Modifies the SPT computation timer.
	timers throttle route inter-area	Modifies the inter-area route computation delay.
	timers throttle route ase	Modifies the inter-area route computation delay.

6.4.1 Configuring OSPF Basic Functions

Configuration Effect

- Set up an OSPF routing domain on the network to provide IPv6 unicast routing service for users on the network.

Notes

- Ensure that the IPv6 routing function is enabled, that is, **ipv6 routing** is not disabled; otherwise, OSPF cannot be enabled.
- IPv6 must be enabled on the interface.
- It is strongly recommended that you manually configure the router ID.

Configuration Steps

Creating an OSPF Process

- Mandatory.
- The configuration is mandatory for every router.

Configuring a Router ID

- (Optional) It is strongly recommended that you manually configure the router ID.
- If the router ID is not configured, OSPF selects an interface IP address. If the IP address is not configured for any interface, or the configured IP addresses have been used by other OSPF instances, you must manually configure the router ID.

Enabling OSPF on an Interface and Specifying an Area ID

- Mandatory.
- The configuration is mandatory for every router.

Verification

- Run the **show ipv6 route ospf** command to verify that the entries of the OSPF routing table are correctly loaded.
- Run the **ping** command to verify that the IPv6 unicast service is correctly configured.

Related Commands

Creating an OSPF Process

Command	**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]
Parameter Description	*process-id:* Indicates the OSPFv3 process ID. If the process ID is not specified, process 1 is enabled. *vrf-name:* Specifies the VPN routing and forwarding (VRF) to which the OSPFv3 process belongs.
Command Mode	Global configuration mode
Usage Guide	After enabling the OSPFv3 process, the device enters the routing process configuration mode.

Configuring a Router ID

Command	**router-id** *router-id*
Parameter Description	*router-id:* Indicates the ID of the device, which is expressed in the IPv4 address.
Command Mode	OSPF routing process configuration mode
Usage Guide	Every device where OSPFv3 run must be identified by using a router ID. You can configure any IPv4 address as the router ID of the device, and ensure that the router ID is unique in an AS. If multiple OSPFv3 processes run on the same device, the router ID of each process must also be unique. After the router ID changes, OSPF performs a lot of internal processing. Therefore, you are advised not to change the router ID unless necessary. When an attempt is made to modify the router ID, a prompt is displayed, requesting you to confirm the modification. After the OSPFv3 process is enabled, you are advised to specify the router ID before configuring other parameters of the process.

Enabling OSPF on an Interface and Specifying an Area ID

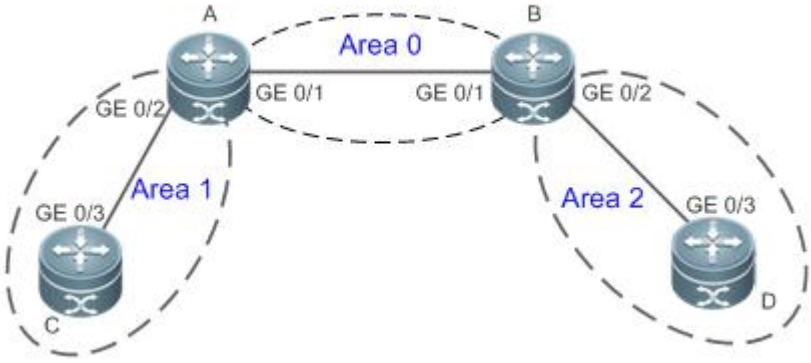
Command	**ipv6 ospf** *process-id* **area** *area-id* [**instance** *instance-id*]
Parameter Description	*process-id*: Indicates the ID of an OSPFv3 process. The value ranges from 1 to 65,535. **Area** *area-id:* Indicates the ID of the OSPFv3 area in which the interface participates. It can be an integer or an IPv4 prefix. **Instance** *instance-id:* Indicates the ID of a specified OSPFv3 process of the interface. The value ranges from 0 to 255.
Command Mode	Interface configuration mode
Usage Guide	Run this command in interface configuration mode to enable the interface to participate in OSPFv3, and then run the **ipv6 router ospf** command to configure the OSPFv3 process. After the OSPFv3 process is configured, the interface will automatically participate in the related process. Run the **no ipv6 ospfarea** command so that the specified interface no longer participates in the OSPFv3 routing process. Run the **no ipv6 router ospf** command so that all interfaces no longer participate in the OSPFv3 routing process. The adjacency can be set up only between devices with the same *instance-id*. After this command is configured, all prefix information on the interface will participate in the OSPFv3 process.

Creating a Virtual Link

Command	**area** *area-id* **virtual-link***router-id* [**hello-interval** *seconds*] [**dead-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**instance** *instance-id*] [**authenticationipsec spi***spi*[**md5|sha1**] [**0|7**] *key*] [**encryption ipsec spi***spi* **esp** [**null**|[**des | 3des**] [**0** | **7**]*des-key*][**md5|sha1**] [**0|7**] *key*]
Parameter Description	*area-id:* Indicates the ID of the area where the virtual link is located. It can be an integer or an IPv4 prefix. *router-id:* Indicates the router ID of the neighbor connected to the virtual link. **dead-interval***seconds:* Indicates the time that the local interface of the virtual link detects the failure of the neighbor. The unit is second. The value ranges from 1 to 65,535. **hello-interval** *seconds:* Indicates the time that the Hello packet is sent on the local interface of the virtual link. The unit is second. The value ranges from 1 to 65,535. **retransmit-interval** *seconds:* Indicates the interval at which the LSA is retransmitted on the local interface of the virtual link. The unit is second. The value ranges from 1 to 65,535. **transmit-delay** *seconds:* Indicates the delay after which the LSA is sent on the local interface of the virtual link. The unit is second. The value ranges from 1 to 65,535. **instance***instance-id:* Indicates the ID of the instance corresponding to the virtual link. The value ranges from 0 to 255. A virtual link cannot be set up between devices with different instance IDs. *spi:* Indicates the security parameter index (SPI). The value ranges from 256 to 4,294,967,295. md5: Enables message digit 5 (MD5) authentication. sha1: Enables Secure Hash Algorithm 1 (SHA1) authentication. 0: Indicates that the key is displayed in plain text. 7: Indicates that the key is displayed in cipher text. *key:* Indicates the authentication key. **null:** Indicates that no encryption mode is used. **des:** Specifies the DES encryption mode. **3des:** Specifies the 3DES encryption mode. *des-key:* Indicates the encryption key.
Command Mode	OSPF routing process configuration mode
Usage Guide	In an OSPFv3 AS, all areas must be connected to the backbone area to properly learn the routing information of the entire OSPFv3 AS. If an area cannot be directly connected to the backbone area, the virtual link can be used to connect this area to the backbone area. The area where the virtual link is located cannot be a stub or NSSA area. At both ends of neighbors between which the virtual link is set up, settings of **hello-interval, dead-interval**, and **instance** must be consistent; otherwise, the adjacency cannot be set up properly.

Configuration Example

Scenario



Remarks	The interface IP addresses are as follows: A: GE 0/1 2001:1::1/64 GE 0/2 2001:2::1/64 B: GE 0/1 2001:1::2/64 GE 0/2 2001:3::1/64 C: GE 0/3 2001:2::2/64 D: GE 0/3 2001:3::2/64

Configuration Steps

- Configure the interface IP addresses on all routers.
- Enable the IPv4 unicast routing function on all routers. (This function is enabled by default.)
- Configure the OSPF instances and router IDs on all routers.
- Enable OSPF on the interfaces configured on all routers.

A

```
A#configure terminal
A(config)#interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)#ipv6 enable
A(config-if-GigabitEthernet 0/1)#ipv6 address 2001:1::1/64
A(config-if-GigabitEthernet 0/1)#ipv6 ospf 1 area 0
A(config-if-GigabitEthernet 0/1)#exit
A(config)#interface GigabitEthernet 0/2
A(config-if-GigabitEthernet 0/2)#ipv6 enable
A(config-if-GigabitEthernet 0/2)#ipv6 address 2001:2::1/64
A(config-if-GigabitEthernet 0/2)#ipv6 ospf 1 area 1
A(config-if-GigabitEthernet 0/2)#exit
A(config)#ipv6 router ospf 1
A(config-router)#router-id1.1.1.1
```

B

```
B#configure terminal
B(config)#interface GigabitEthernet 0/1
B(config-if-GigabitEthernet 0/1)#ipv6 enable
B(config-if-GigabitEthernet 0/1)#ipv6 address 2001:1::2/64
B(config-if-GigabitEthernet 0/1)#ipv6 ospf 1 area 0
B(config-if-GigabitEthernet 0/1)#exit
```

	B(config)#interface GigabitEthernet 0/2 B(config-if-GigabitEthernet 0/2)#ipv6 enable B(config-if-GigabitEthernet 0/2)#ipv6 address 2001:3::1/64 B(config-if-GigabitEthernet 0/2)#ipv6 ospf 1 area 2 B(config-if-GigabitEthernet 0/2)#exit B(config)#ipv6 router ospf 1 B(config-router)#router-id2.2.2.2
C	C#configure terminal C(config)#interface GigabitEthernet 0/3 C(config-if-GigabitEthernet 0/3)#ipv6 enable C(config-if-GigabitEthernet 0/3)#ipv6 address 2001:2::2/64 C(config-if-GigabitEthernet 0/3)#ipv6 ospf 1 area 1 C(config-if-GigabitEthernet 0/3)#exit C(config)#ipv6 router ospf 1 C(config-router)#router-id3.3.3.3
D	D#configure terminal D(config)#interface GigabitEthernet 0/3 D(config-if-GigabitEthernet 0/3)#ipv6 enable D(config-if-GigabitEthernet 0/3)#ipv6 address 2001:4::2/64 D(config-if-GigabitEthernet 0/3)#ipv6 ospf 1 area 2 D(config-if-GigabitEthernet 0/3)#exit D(config)#ipv6 router ospf 1 D(config-router)#router-id4.4.4.4
Verification	● Verify that the OSPF neighbors are correct on all routers. ● Verify that the routing table is correctly loaded on all routers. ● Verify that 2001:2::2/64 can be pinged successfully on Router D.
A	A#show ipv6 ospf neighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Instance ID Interface 2.2.2.2 1 Full/BDR 00:00:30 0 GigabitEthernet 0/1 3.3.3.31 Full/BDR 00:00:35 0 GigabitEthernet 0/2 A#show ipv6 route ospf

	IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area O IA2001:3::/64 [110/20] via FE80::2D0:F8FF:FE22:4524, GigabitEthernet 0/1
B	B# show ipv6 ospf neighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Instance ID Interface 1.1.1.11 Full/DR 00:00:30 0 GigabitEthernet 0/1 4.4.4.41 Full/BDR 00:00:35 0 GigabitEthernet 0/2 B#show ipv6 route ospf IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area O IA2001:2::/64 [110/20] via FE80::2D0:F8FF:FE22:4536, GigabitEthernet 0/1
C	C# show ipv6 ospf neighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Instance ID Interface 1.1.1.11 Full/DR 00:00:30 0 GigabitEthernet 0/3 C#show ipv6 route ospf

	IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area O IA2001:1::/64 [110/2] via FE80::2D0:F8FF:FE22:4537, GigabitEthernet 0/3 O IA2001:3::/64 [110/3] via FE80::2D0:F8FF:FE22:4537, GigabitEthernet 0/3
D	D# show ipv6 ospf neighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Instance ID Interface 2.2.2.2 1 Full/DR 00:00:30 0 GigabitEthernet 0/3 D#show ipv6 route ospf IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area O IA2001:1::/64 [110/2] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/3 O IA2001:2::/64 [110/3] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/3 D# D#ping 2001:2::2 Sending 5, 100-byte ICMP Echoes to 2001:2::2, timeout is 2 seconds: < press Ctrl+C to break > !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 5/9/14 ms.

Common Errors

- IPv6 is disabled on the interface.
- OSPF cannot be enabled because the IPv6 unicast routing function is disabled.
- The area IDs enabled on adjacent interfaces are inconsistent.
- The same router ID is configured on multiple routers, resulting in a router ID conflict.

6.4.2 Setting the Network Type

Configuration Effect

- If the physical network is X.25, Frame Relay, or ATM, OSPF can also run to provide the IPv6 unicast routing service.

Notes

- The OSPF basic functions must be configured.
- The broadcast network sends multicast OSPF packets, automatically discovers neighbors, and elects a DR and a BDR.
- The P2P network sends multicast OSPF packets and automatically discovers neighbors.
- The NBMA network sends unicast OSPF packets. Neighbors must be manually specified, and a DR and a BDR must be elected.
- The P2MP network (without carrying the **non-broadcast** parameter) sends multicast OSPF packets. Neighbors are automatically discovered.
- The P2MP network (carrying the **non-broadcast** parameter) sends unicast OSPF packets. Neighbors must be manually specified.

Configuration Steps

Configuring the Interface Network Type

- Optional.
- Perform this configuration on routers at both ends of the link.

Configuring a Neighbor

- (Optional)If the interface network type is set to NBMA or P2MP (carrying the **non-broadcast** parameter), neighbors must be configured.
- Neighbors are configured on routers at both ends of the NBMA or P2MP (carrying the **non-broadcast** parameter) network.

Configuring the Interface Priority

- (Optional)You must configure the interface priority if a router must be specified as a DR, or a router cannot be specified as a DR.
- Configure the interface priority on a router that must be specified as a DR, or cannot be specified as a DR.

Verification

- Run the **show ipv6 ospf interface** command to verify that the network type of each interface is correct.

Related Commands

Configuring the Interface Network Type

Command	**ipv6 ospf network** {**broadcast** | **non-broadcast** |**point-to-point** | **point-to-multipoint**[**non-broadcast**]}[**instance***instance-id*]
Parameter Description	**broadcast**: Indicates the broadcast network type. **non-broadcast:** Indicates the non-broadcast network type. **point-to-multipoint**: Indicates the point-to-multipoint (P2MP) network type. **point-to-multipoint non-broadcast:** Indicates the P2MP non-broadcast network type. **point-to-point:** Indicates the point-to-point (P2P) network type. **instance***instance-id:* Indicates the ID of a specified OSPFv3 process of the interface. The value ranges from 0 to 255.
Command Mode	Interface configuration mode
Usage Guide	You can configure the network type of an interface based on the actual link type and topology.

Configuring a Neighbor

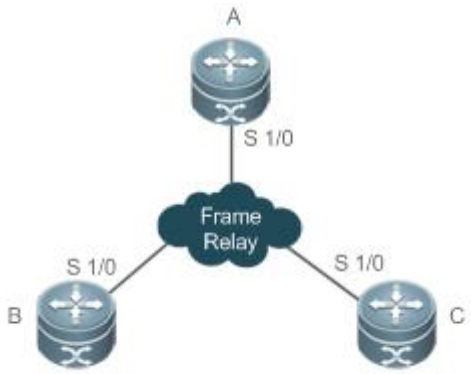
Command	**ipv6 ospf neighbor** *ipv6-address*{ [**cost***cost*] | [**poll-interval***seconds* | **priority***value*] }[**instance***instance-id*]
Parameter Description	*ip-address*: Indicates the link address of theneighborinterface. **cost***cost*: Indicates the cost required from the P2MP network to each neighbor. The cost is not defined by default. The cost configured on the interface is used. The value ranges from 1 to 65,535. Only a P2MP network supports this option. **poll-interval** *seconds*: Indicates the neighbor polling interval. The unit is second. The value ranges from 1 to 2,147,483,647. Only the non-broadcast (NBMA) network supports this option. **priority** *value*: Indicates the priority value of the non-broadcast network neighbor. The value ranges from 0 to 255. Only the non-broadcast network (NBMA) supports this option. **instance***instance-id:* Indicates the ID of a specified OSPFv3 process of the interface. The value ranges from 0 to 255.
Command Mode	Interface configuration mode
Usage Guide	You can configure neighbor parameters based on the actual network type.

Configuring the Interface Priority

Command	**ipv6 ospf priority** *number-value*[**instance***instance-id*]
Parameter Description	*number-value*: Indicates the priority of the interface. The value ranges from 0 to 255. **instance***instance-id:* Indicates the ID of a specified OSPFv3 process of the interface. The value ranges from 0 to 255.
Command Mode	Interface configuration mode
Usage Guide	On a broadcast network, a DR or BDR must be elected. During the DR/BDR election, the device with a higher priority will be preferentially elected as a DR or BDR. If the priority is the same, the device with a larger router ID will be preferentially elected as a DR or BDR. A device with the priority 0 does not participate in the DR/BDR election.

Configuration Example

Configuring the Interface Network Type

Scenario	
Configuration Steps	● Enable IPv6 on interfaces of all routers. ● Configure the OSPF basic functions on all routers. ● Set the interface network type to P2MP on all routers.
A	A#configure terminal A(config)# interface Serial1/0 A(config-Serial1/0)# encapsulation frame-relay A(config-Serial1/0)# ipv6 ospf network point-to-multipoint
B	B#configure terminal B(config)# interface Serial1/0 B(config-Serial1/0)# encapsulation frame-relay B(config-Serial1/0)# ipv6 ospf network point-to-multipoint
C	C#configure terminal C(config)# interface Serial1/0 C(config-Serial1/0)# encapsulation frame-relay C(config-Serial1/0)# ipv6 ospf network point-to-multipoint
Verification	● Verify that the interface network type is P2MP.

A	A#show ipv6 ospf interface Serial1/0 Serial1/0 is up, line protocol is up Interface ID 2 IPv6 Prefixes fe80::2d0:f8ff:fe22:3346/64 (Link-Local Address) OSPFv3 Process (1), Area 0.0.0.1, Instance ID 0 Router ID 192.168.22.30,Network Type POINTOMULTIPOINT, Cost: 1 Transmit Delay is 1 sec, State Point-To-Point, Priority 1 Timer interval configured, Hello 30, Dead 120, Wait 40, Retransmit 10 Hello due in 00:00:06 Neighbor Count is 1, Adjacent neighbor count is 1 Hello received 40 sent 40, DD received 17 sent 9 LS-Req received 1 sent 3, LS-Upd received 6 sent 5 LS-Ack received 3 sent 4, Discarded 1

Common Errors

- The network types configured on interfaces at two ends are inconsistent, causing abnormal route learning.
- The network type is set to NBMA or P2MP (non-broadcast), but neighbors are not specified.

6.4.3 Configuring Route Redistribution and Default Route

Configuration Effect

- Introduce unicast routes for other AS domains to the OSPF domain to provide the unicast routing service to other AS domains for users in the OSPF domain.
- In the OSPF domain, inject a default route to another AS domain so that the unicast routing service to another AS domain can be provided for users in the OSPF domain.

Notes

- The OSPF basic functions must be configured.

Configuration Steps

Configuring External Route Redistribution

- (Optional)This configuration is mandatory if external routes of the OSPF domain should be introduced to the ASBR.
- Perform this configuration on an ASBR.

Generating a Default Route

- (Optional)Perform this configuration if the default route should be introduced to an ASBR so that other routers in the OSPF domain access other AS domains through this ASBR by default.

- Perform this configuration on an ASBR.

Verification

- On a router inside the OSPF domain, run the **show ipv6 route ospf** command to verify that the unicast routes to other AS domains are loaded.
- On a router inside the OSPF domain, run the **show ipv6 route ospf** command to verify that the default route to the ASBR is loaded.
- Run the **ping** command to verify that the IPv6 unicast service to other AS domains is correct.

Related Commands

Configuring Route Redistribution

Command	**redistribute** {**bgp** | **connected** |**isis**[*area-tag*] |**ospf***process-id*| **rip** | **static**}[{**level-1** | **level-1-2** | **level-2**} | **match** {**internal** | **external** [**1**|**2**]**nssa-external** [**1**|**2**]} | **metric** *metric-value*|**metric-type** {**1**|**2**} | **route-map** *route-map-name* |**tag***tag-value*]
Parameter Description	**bgp:** Indicates redistribution from BGP. **connected:** Indicates redistribution from direct routes. **isis** [*area-tag*]: Indicates redistribution from IS-IS.**area-tag** specifies the IS-IS instance. **ospf***process-id:* Indicates redistribution from OSPF.**process-id** specifies an OSPF instance. The value ranges from 1 to 65535. 1-65535 **rip:** Indicates redistribution from RIP. **static:** Indicates redistribution from static routes. **level-1** | **level-1-2** | **level-2:** Used only when IS-IS routes are redistributed. Only the routes of the specified level are redistributed. By default, only level-2 IS-IS routes can be redistributed. **match:** Used only when OSPF routes are redistributed. Only the routes that match the specified criteria are redistributed. By default, all OSPF routes can be redistributed. **metric***metric-value:* Indicates the metric of the OSPF external LSA. *metric-value* specifies the size of the metric. The value ranges from 0 to 16,777,214. **metric-type** {**1**|**2**}: Indicates the external route type, which can be E-1 or E-2. **route-map***route-map-name:* Sets the redistribution filtering rules. **tag***tag-value:* Specifies the tag value of the route that is redistributed into the OSPF routing domain. The value ranges from 0 to 4294967295.
Command Mode	OSPF routing process configuration mode
Usage Guide	When the device supports multiple routing protocols, collaboration between protocols is very important. To run multiple routing protocols concurrently, the device must be able to redistribute routing information of a protocol to another protocol. This applies to all routing protocols. During redistribution of IS-IS routes, **level-1**,**level-2**, or **level-1-2** can be configured to indicate that IS-IS routes of the specified level(s) will be redistributed. By default, IS-IS routes of level 2 are redistributed. During redistribution of OSPFv3 routes, **match** can be configured to indicate that OSPFv3 routes of the specified sub-type will be redistributed. By default, all types of OSPFv3 routes are redistributed. For the **level** parameter configured during redistribution of IS-IS routes and the match parameter configured during redistribution of OSPFv3 routes, the routes are matched against the route map only when the sub-type of the routes are correct. During configuration of route redistribution, the **match**rules configured in route map configuration mode areused based

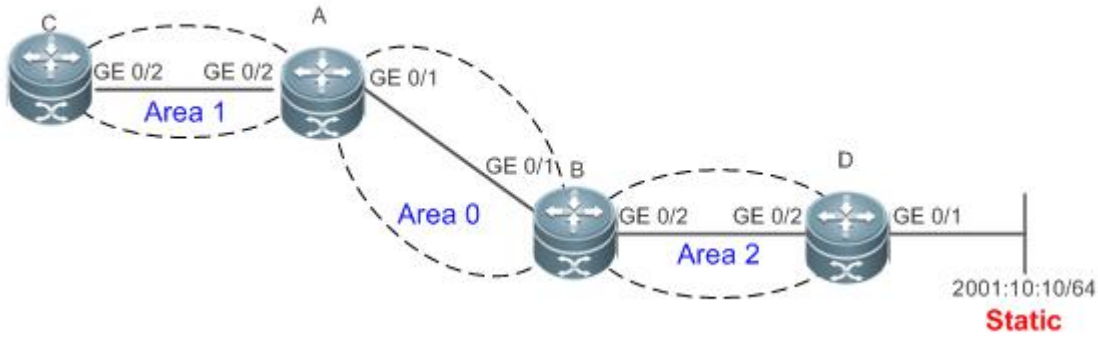
	on the original information of routes. The priorities of **tag**, **metric** and **metric-type** in the route redistribution configuration are lower than the priority of the**set** rulesconfigured in route map configuration mode. The **set metric** value of the associated routemap should fall into the range of 0 to 16,777,214. If the value exceeds this range, routes cannot be introduced. The configuration rules for the **no** form of the **redistribute** command are as follows: 1. If some parameters are specified in the **no** form of the command, default values of these parameters will be restored. 2. If no parameter is specified in the **no** form of the command, the entire command will be deleted. For example, if **redistribute isis 112 level-2** is configured, the **no redistribute isis 112 level-2** command only restores the default value of **level-2**. As level-2 itself is the default value of the parameter, the configuration saved is still **redistribute isis 112 level-2** after the preceding no form of the command is executed. To delete the entire command, you need to run the **no redistribute isis 112** command.

Introducing a Default Route

Command	**default-information originate** [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map***map*]
Parameter Description	**always:** Enables OSPF to generate a default route regardless of whether the local router has a default route. **metric** *metric:* Indicates the initial metric of the default route. The value ranges from 0 to 16,777,214. By default, the metric of the default route is 1. **metric-type***type:* Indicates the type of the default route. OSPF external routes are classified into two types: Type 1: The metric varies with routers; Type 2: The metric is the same for all routers. Type 1 external routes are more trustworthy than Type 2 external routes. **route-map** *map-name:* Indicates the associated route-map name. By default, no route-map is associated.
Command Mode	OSPF routing process configuration mode
Usage Guide	When the **redistribute** or **default-information** command is executed, the OSPFv3-enabled router automatically becomes an ASBR. The ASBR, however, does not automatically generate or advertise a default route to all routers in the OSPF routing domain. To have the ASBR generate a default route, configure the **default-information originate** command. If **always** is specified, the OSPFv3 process advertises an external default route to neighbors no matter whether a default route exists in the core routing table. This default route, however, is not displayed on the local router. To confirm whether the default route is generated, run the **show ipv6 ospf database** command to display the OSPFv3 link status database. On an OSPFv3 neighbor, you can run the **show ipv6 route ospf** command to see the default route. The metric of the external default route can only be defined in the **default-information originate** command, instead of the **default-metric** command. OSPFv3 has two types of external routes. The metric of the Type 1 external route changes, but the metric of the Type 2 external route is fixed. If two parallel paths to the same destination network have the same route metric, the priority of the Type 1 route is higher than that of the Type 2 route. Therefore, the **show ipv6 route ospf** command displays only the Type 1 route. A router in a stub area cannot generate an external default route.

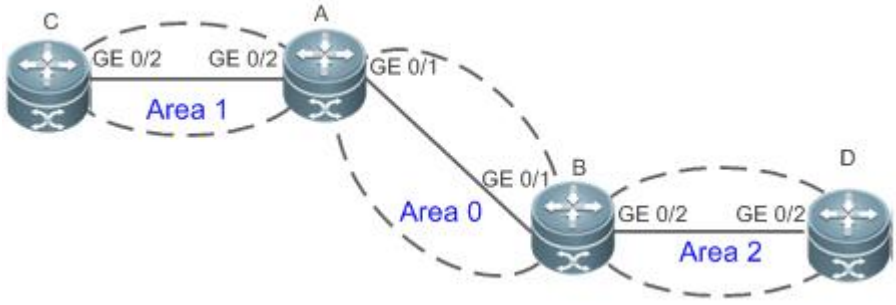
Configuration Example

Configuring Route Redistribution

Scenario	
Configuration Steps	● Enable IPv6 on interfaces of all routers. ● Configure the OSPF basic functions on all routers. ● Introduce an external static route to Router D.
D	D#configure terminal D(config)#ipv6 router ospf 1 D(config-router)# redistribute static
Verification	● On Router D, run the **show ipv6ospf database external brief** command to verify that an LSA corresponding to an external route is generated. ● On Router C, run the **show ipv6 route ospf** command to verify that the external static route has been introduced.
D	D#show ipv6 ospf database external OSPFv3 Router with ID (4.4.4.4) (Process 1) AS-external-LSA LS age: 7 LS Type: AS-External-LSA Link State ID: 0.0.0.6 Advertising Router: 4.4.4.4 LS Seq Number: 0x80000001 Checksum: 0x9C1F Length: 36 Metric Type: 2 (Larger than any link state path) Metric: 20 Prefix: 2001:10:10::/64 Prefix Options: 0 (-|-|-|-)

C	C#show ipv6 route ospf IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area O E2 2001:10:10::/64 [110/20] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/2

Configuring the Default Route

Scenario	
Configuration Steps	● Enable IPv6 on interfaces of all routers. ● Configure the OSPF basic functions on all routers. ● Configure the default route on Router D.
D	D#configure terminal D(config)#ipv6 router ospf 1 D(config-router)#default-information originate always
Verification	● On Router D, run the **show ipv6ospf database external brief** command to verify that an LSA corresponding to the default route is generated. ● On Router C, run the **show ipv6 route ospf** command to verify that the OSPF default route exists.

D	D#show ipv6 ospf database external OSPFv3 Router with ID (4.4.4.4) (Process 1) AS-external-LSA LS age: 3 LS Type: AS-External-LSA Link State ID: 0.0.0.7 Advertising Router: 4.4.4.4 LS Seq Number: 0x80000001 Checksum: 0x1839 Length: 32 Metric Type: 2 (Larger than any link state path) Metric: 1 Prefix: ::/0 Prefix Options: 0 (-|-|-|-) External Route Tag: 1
C	C#show ipv6route ospf IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area O E2::/0 [110/20] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/2

Common Errors

- A route loop is formed because the **default-information originate always** command is configured on multiple routers.
- Routes cannot be introduced because route redistribution is configured on a router in the stub area.

6.4.4 Configuring the Stub Area and NSSA Area

Configuration Effect

- Configure an area located on the stub as a stub area to reduce interaction of routing information and the size of routing table, and enhance stability of routes.

Notes

- The OSPF basic functions must be configured.
- A backbone or transit area cannot be configured as a stub or an NSSA area.
- A router in the stub area cannot introduce external routes, but a router in the NSSA area can introduce external routes.

Configuration Steps

Configuring a Stub Area

- (Optional)Perform this configuration if you wish to reduce the size of the routing table on routers in the area.
- Perform this configuration on all routers in the same area.

Configuring an NSSA Area

- (Optional)Perform this configuration if you wish to reduce the size of the routing table on routers in the area and introduce OSPF external routes to the area.
- The area must be configured as an NSSA area on all routers in this area.

Verification

Verifying the Stub Area

- On a router in the stub area, run the **show ipv6 route** command to verify that the router is not loaded with any external routes.

Verifying the NSSA Area

- On a router in the NSSA area, run the **show ipv6 ospf database** command to verify that the introduced external route generates Type 7 LSAs.
- On a router in the backbone area, run the **show ipv6 route** command to verify that the router is loaded with external routes introduced from the NSSA area.

Related Commands

Configuring a Stub Area

Command	**area***area-id***stub** [**no-summary**]
Parameter Description	*area-id:* Indicates the ID of the stub area. The value can be an integer or an IPv4 prefix. **no-summary:** This option is valid only ona the ABR in a stub area. If this option is specified, the ABR only advertises one Type 3 LSA indicating the default route to the stub area, and does not advertise other Type 3 LSAs.
Command Mode	OSPF routing process configuration mode
Usage Guide	An area located on the stub of a network can be configured as a stub area. You must run the **area stub** command on all routers in a stub area. Devices in a stub area cannot learn the external routes (Type 5 LSAs) of the AS. In practice, external routes take up a large proportion of the link status database. Therefore, devices in a stub area can learn only a small amount of routing information, which reduces the amount of system resources required to run the OSPFv3 protocol. By default, an ABR in a stub area will generate a Type 3 LSA indicating the default fault, and advertise the LSA to the stub

	area. In this way, devices in the stub area can access devices outside the AS. To configure a totally stub area, add the **no-summary** keyword when running the **area stub** command on the ABR.

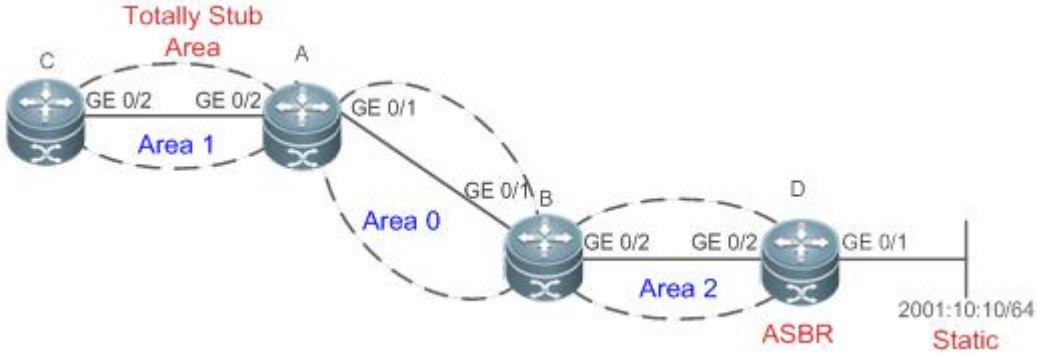
Configuring an NSSA Area

Command	**area***area-id* **nssa** [**no-redistribution**] [**default-information-originate**[**metric***value*] [**metric-type***type*]] [**no-summary**] [**translator** [**stability-interval***seconds* | **always**]] [**translate type7 suppress-fa**] [**zero-address-forwarding**]
Parameter Description	*area-id:* Indicates the ID of the NSSA area. **no-redistribution:** Select this option if the router is an NSSA ABR and you want to use only the **redistribute** command to introduce the routing information into a common area instead of an NSSA area. **default-information-originate:** Indicates that a default Type 7 LSA is generated and introduced to the NSSA area. This option takes effect only on an NSSA ABR or ASBR. **metric***value:* Specifies the metric of the generated default LSA. The value ranges from 0 to 16,777,214. The default value is 1. **metric-type***type:* Specifies the route type of the generated default LSA. The values include 1 and 2. **1** represents N-1, and **2** represents N-2. The default value is 2. **no-summary:** Prohibits the ABR in the NSSA area from sending summary LSAs (Type-3 LSA). **translator:** Indicates that the NSSA ABR is a translator. **stability-interval***seconds:* Indicates the stability interval after the NSSA ABR is changed from a translator to a non-translator. The unit is second. The default value is 40. The value ranges from 0 to 2,147,483,647. **always:** Indicates that the current NSSA ABR always acts as a translator. The default value is the standby translator. **translate type7 suppress-fa:** Indicates that the Type 5 LSA does not carry the forwarding address (FA) when the Type 7 LSA is converted to the Type 5 LSA. **zero-address-forwarding:** When importing external routes to NSSA ABR, FA of NSSA LSA is set as 0.0.0.0.
Command Mode	OSPF routing process configuration mode
Usage Guide	The **default-information-originate** parameter is used to generate a default Type 7 LSA. This parameter has different functions on the ABR and the ASBR in the NSSA area. On the ABR, a Type 7 LSA default route is generated regardless of whether the default route exists in the routing table. On the ASBR (not an ABR), a Type 7 LSA default route is generated only when the default route exists in the routing table. If the **no-redistribution** parameter is configured on the ASBR, other external routes introduced by OSPF through the **redistribute** command cannot be advertised to the NSSA area. This parameter is generally used when a router in the NSSA area acts both as the ASBR and the ABR. It prevents external routing information from entering the NSSA area. To further reduce the number of LSAs sent to the NSSA area, you can configure the **no-summary** parameter on the ABR to prevent the ABR from sending the summary LSAs (Type 3 LSA) to the NSSA area. **area default-cost** is used on an ABR or ASBR connected to the NSSA area. This command configures the cost of the default route sent from the ABR/ASBR to the NSSA area. By default, the cost of the default route sent to the NSSA area is 1. If an NSSA area has two or more ABRs, the ABR with the largest router ID is elected by default as the translator for converting Type 7 LSAs into Type 5 LSAs. If the current device is always the translator ABR for converting Type 7 LSAs into Type 5 LSAs, use the **translator always** parameter. If the translator role of the current device is replaced by another ABR, the conversion capability is retained during the time specified by **stability-interval**. If the router does not become a translator again during **stability-interval**, LSAs that are converted from Type 7 to Type 5 will be deleted from the AS after **stability-interval** expires. To prevent a routing loop, LSAs that are converted from Type 7 to Type 5 will be deleted from the AS immediately after

	the current device loses the translator role even if **stability-interval** does not expire. In the same NSSA area, it is recommended that **translator always** be configured on only one ABR.

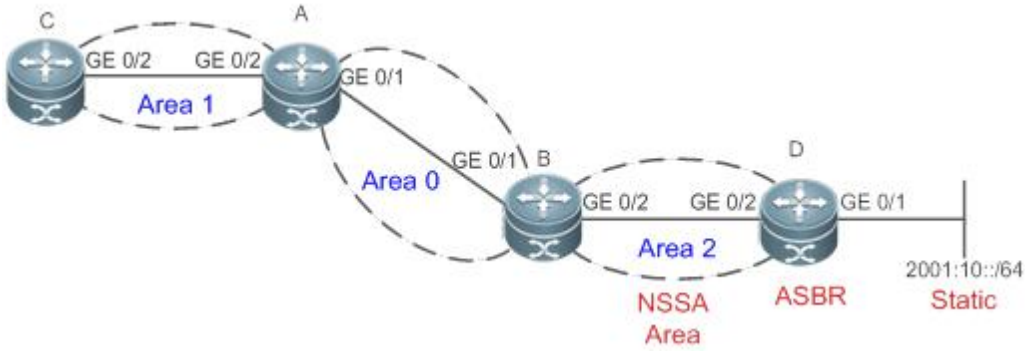
Configuration Example

Configuring a Stub Area

Scenario	
Configuration Steps	● Enable IPv6 on interfaces of all routers.(Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Introduce an external static route to Router D. ● Configure area 1 as the stub area on Router A and Router C.
D	D#configure terminal D(config)#ipv6 router ospf 1 D(config-router)#redistribute static
A	A# configure terminal A(config)#ipv6 router ospf 1 A(config-router)#area 1 stubno-summary
C	C#configure terminal C(config)#ipv6 router ospf 1 C(config-router)#area 1 stub
Verification	● On Router C, run the **show ipv6 route ospf** command to display the routing table. Verify that there is only one default inter-area route, and no external static route is introduced from Router D.

C	C#show ipv6 route ospf IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area O IA::/0 [110/3] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/2

Configuring an NSSA Area

Scenario	
Configuration Steps	• Enable IPv6 on interfaces of all routers.(Omitted) • Configure the OSPF basic functions on all routers. (Omitted) • Introduce an external static route to Router D. • Configure area 1 as the NSSA area on Router B and Router D.
D	D#configure terminal D(config)#ipv6 router ospf 1 D(config-router)#area 1 nssa D(config-router)#redistribute static
B	B#configure terminal B(config)#ipv6 router ospf 1 B(config-router)#area 1 nssa
Verification	• On Router D, run the **show ipv6 ospf database** command to display the database information and verify that Type 7 LSAs are generated. • On Router A, run the **show ipv6 route ospf** command to display the routing table and verify that an external static route is introduced by Router D.

D	D#show ipv6 ospf database nssa-external OSPFv3 Router with ID (1.1.1.1) (Process 1) NSSA-external-LSA (Area 0.0.0.1) LS age: 1196 LS Type: NSSA-external-LSA Link State ID: 0.0.0.3 Advertising Router: 1.1.1.1 LS Seq Number: 0x80000004 Checksum: 0x1F25 Length: 52 Metric Type: 2 (Larger than any link state path) Metric: 20 Prefix: 2001:10::/64 Prefix Options: 8 (P|-|-|-) Forwarding Address: 4000::1
A	A#show ipv6 route ospf IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area O N2 2001:10::/64 [110/20] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/1

Common Errors

- Configurations of the area type are inconsistent on routers in the same area.
- External routes cannot be introduced because route redistribution is configured on a router in the stub area.

6.4.5 Configuring Route Summarization

Configuration Effect

- Summarize routes to reduce interaction of routing information and the size of routing table, and enhance stability of routes.

- Shield or filter routes.

Notes

- The OSPF basic functions must be configured.
- The address range of the summarize route may exceed the actual network range in the routing table. If data is sent to a network beyond the summarization range, a routing loop may be formed and the router processing load may increase. To prevent these problems, a discard route must be added to the routing table or shield or filter routes.

Configuration Steps

Configuring Inter-Area Route Summarization

- (Optional) Perform this configuration when routes of the OSPF area need to be summarized.
- Unless otherwise required, perform this configuration on an ABR in the area where routes to be summarized are located.

Configuring External Route Summarization

- (Optional) Perform this configuration when routes external to the OSPF domain need to be summarized.
- Unless otherwise required, perform this configuration on an ASBR, to which routes that need to be summarized are introduced.

Verification

- Run the **show ipv6 route ospf** command to verify that individual routes do not exist and only the summarized route exists.

Related Commands

Configuring Inter-Area Route Summarization

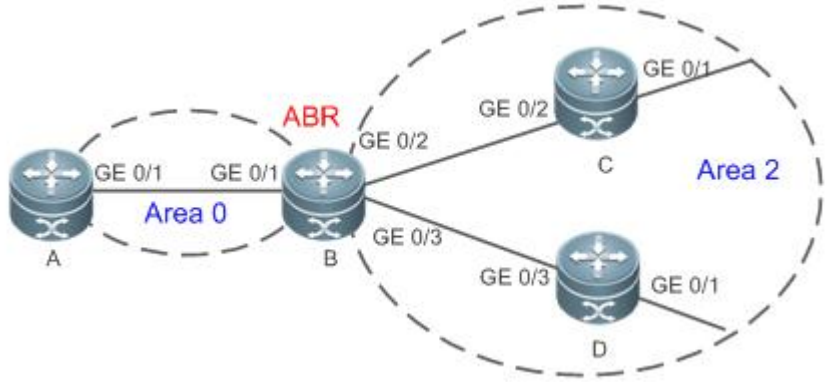
Command	**area***area-id***range***ipv6-prefix/prefix-length* [**advertise**|**not-advertise**]
Parameter Description	*area-id*: Specifies the ID of the OSPF area to which the summarized route should be injected. The value can be an integer or an IPv4 prefix. *ipv6-prefix/prefix-length*: Indicates the range of IP addresses to be summarized. **advertise** | **not-advertise**: Specifies whether the summarized route should be advertised.
Command Mode	OSPF routing process configuration mode
Usage Guide	This command takes effect only on an ABR, and is used to summarize multiple routes in an area into a route and advertise this route to other areas. Combination of the routing information occurs only on the boundary of an area. Routers inside the area can learn specific routing information, whereas routers in other areas can learn only one summarized route. In addition, you can set **advertise** or **not-advertise** to determine whether to advertise the summarized route to shield and filter routes. By default, the summarized route is advertised. You can use the **cost** parameter to set the metric of the summarized route. You can configure route summarization commands for multiple areas. This simplifies routes in the entire OSPF routing domain, and improves the network forwarding performance, especially for a large-sized network. When multiple route summarization commands are configured and have the inclusive relationship with each other, the area range to be summarized is determined based on the maximum match principle.

Configuring External Route Summarization

Command	**summary-prefix***ipv6-prefix/prefix-length* [**not-advertise** | **tag** *number*]

Parameter Description	*ipv6-prefix/ prefix-length*: Indicates the range of IP addresses to be summarized. **not-advertise**: Indicates that the summarized route is not advertised. If this parameter is not specified, the summarized route is advertised. **tag***number:* Specifies the tag value of the route that is redistributed into the OSPFv3 routing domain. The value ranges from 0 to 4,294,967,295.
Command Mode	OSPF routing process configuration mode
Usage Guide	When routes are redistributed from other routing processes and injected to the OSPFv3 routing process, each route is advertised to the OSPFv3 routers using an external LSA. If the injected routes are a continuous address space, the ABR can advertise only one summarized route to significantly reduce the size of the routing table. **area range** summarizes the routes between OSPFv3 areas, whereas **summary-prefix** summarizes external routes of the OSPFv3 routing domain. When configured on the NSSA ABR translator, **summary-prefix** summarizes redistributed routes and routes obtained based on the LSAs that are converted from Type 7 to Type 5. When configured on the ASBR (not an NSSA ABR translator), **summary-prefix** summarizes only redistributed routes.

Configuration Example

Configuration Steps	 **Remarks**: The interface IPv6 addresses are as follows: B: GE0/2 2001:16:2::1/64 GE0/3 2001:16:3::1/64 C: GE0/2 2001:16:2::2/64 GE0/1 2001:16:4::2/64 D: GE0/3 2001:16:3::2/64 GE0/1 2001:16:5::1/64
Configuration Steps	• Enable IPv6 on interfaces of all routers.(Omitted) • Configure the OSPF basic functions on all routers. (Omitted) • Summarize routes of area 2 on Router B.
B	B#configure terminal B(config)#ipv6 router ospf 1 B(config-router)#area 2 range 2001:16::/64
Verification	On Router A, check the routing table and verify that the entry 2001:16::/64 is generated and other routes do not exist.

A	A#show ipv6 route ospf IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area O IA 2001:16::/64 [110/2] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/1

Common Errors

- Inter-area route summarization cannot be implemented because the **area range** command is configured on a non-ABR device.

6.4.6 Configuring Route Filtering

Configuration Effect

- Routes that do not meet filtering conditions cannot be loaded to the routing table, or advertised to neighbors. Network users cannot access specified destination network.

Notes

- The OSPF basic functions must be configured.
- Filtering routes by using the **distribute-list in** command affects forwarding of local routes, but does not affect route computation based on LSAs. Therefore, if route filtering is configured on the ABR, Type 3 LSAs will still be generated and advertised to other areas because routes can still be computed based on LSAs. As a result, black-hole routes are generated. In this case, you can run the **area filter-list** or **area range** (containing the **not-advertise** parameter) command on the ABR to prevent generation of black-hole routes.

Configuration Steps

Configuring Inter-Area Route Filtering

- (Optional) This configuration is recommended if users need to be restricted from accessing the network in a certain OSPF area.
- Unless otherwise required, perform this configuration on an ABR in the area where filtered routes are located.

Configuring Redistributed Route Filtering

- (Optional) Perform this configuration if external routes introduced by the ASBR need to be filtered.
- Unless otherwise required, perform this configurationon an ASBR to which filtered routes are introduced.

Configuring Learned Route Filtering

- (Optional) Perform this configuration if users need to be restricted from accessing a specified destination network.
- Unless otherwise required, perform this configurationon a router that requires route filtering.

Verification

- Run the **show ipv6 route** command to verify that the router is not loaded with routes that have been filtered out.
- Run the **ping** command to verify that the specified destination network cannot be accessed.

Related Commands

Configuring a Passive Interface

Command	**passive-interface** {**default** | *interface-typeinterface-number*}
Parameter Description	*interface-type interface-number*: Indicates the interface that should be configured as a passive interface. **default:** Indicates that all interfaces will be configured as passive interfaces.
Command Mode	OSPF routing process configuration mode
Usage Guide	When an interface is configured as a passive interface, it no longer sends or receives Hello packets. This command takes effect only on an OSPFv3-enabled interface, and not on a virtual link.

Configuring Redistributed Route Filtering

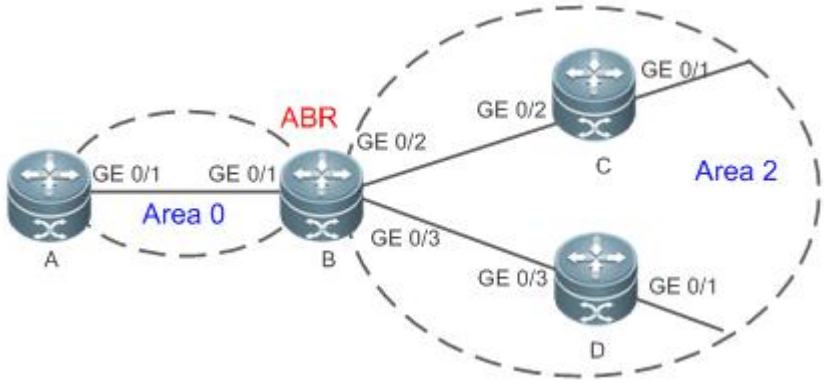
Command	**distribute-list**{*name* | **prefix-list** *prefix-list-name*}**out**[**bgp** | **connected** |**isis**[*area-tag*]| **ospf** *process-id*| **rip** | **static**]
Parameter Description	*name*: Uses the ACL for filtering. **prefix** *prefix-list-name*: Uses the prefix list for filtering. **bgp | connected | isis**[*area-tag*] | **ospf** process-id| **rip** | **static**: Indicates the source of routes to be filtered.
Command Mode	OSPF routing process configuration mode
Usage Guide	**distribute-list out** is similar to **redistribute route-map**, and is used to filter routes that are redistributed from other protocols to OSPFv3. The **distribute-list out** command itself does not redistribute routes, and is generally used together with the **redistribute** command. The ACL and the prefix list filtering rules are mutually exclusive in the configuration. That is, if the ACL is used for filtering routes coming from a certain source, the prefix list cannot be configured to filter the same routes.

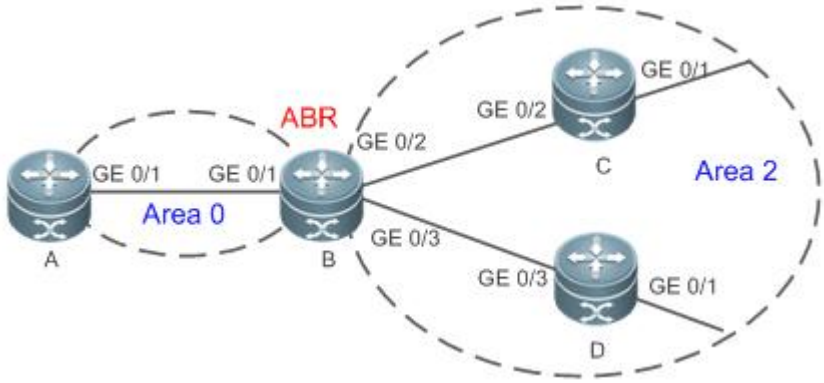
Configuring Learned Route Filtering

Command	**distribute-list**{*name* | **prefix-list** *prefix-list-name*}**in** [*interface-typeinterface-number*]
Parameter Description	*name*: Uses the ACL for filtering. **prefix***prefix-list-name*: Uses the prefix list for filtering. *interface-type interface-number:* Specifies the interface for which LSA routes are filtered.
Command Mode	OSPF routing process configuration mode
Usage Guide	Filter routes that are computed based on received LSAs. Only routes meeting the filtering conditions can be forwarded. The command does not affect the LSDB or the routing tables of neighbors. The ACL and the prefix list filtering rules are mutually exclusive in the configuration. That is, if the ACL is used for filtering routes on a specified interface, the prefix list cannot be configured to filter routes on the same interface. Filtering routes by using the **distribute-list in** command affects forwarding of local routes, but does not affect route

	computation based on LSAs. Therefore, if route filtering is configured on the ABR, Type 3 LSAs will still be generated and advertised to other areas because routes can still be computed based on LSAs. As a result, black-hole routes are generated. In this case, you can run the **area range** (containing the **not-advertise** parameter) command on the ABR to prevent generation of black-hole routes.

Configuration Example

Scenario	 **Remarks** The interface IPv6 addresses are as follows: B: GE0/2 2001:16:2::1/64 GE0/3 2001:16:3::1/64 C: GE0/2 2001:16:2::2/64 GE0/1 2001:16:4::2/64 D: GE0/3 2001:16:3::2/64 GE0/1 2001:16:5::1/64
Configuration Steps	● Enable IPv6 on interfaces of all routers.(Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router A, configure route filtering.
A	A#configure terminal A(config)#ipv6 access-list test A (config-ipv6-acl)#permit ipv6 2001:16:5::/64 any A(config)#ipv6 router ospf 1 A(config-router)#distribute-list test in GigabitEthernet0/1
Verification	● On Router A, check the routing table. Verify that only the entry 2001:16:5::/64 is loaded.
A	A#show ipv6 route ospf IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area

Scenario	 **Remarks**: The interface IPv6 addresses are as follows: B: GE0/2 2001:16:2::1/64 GE0/3 2001:16:3::1/64 C: GE0/2 2001:16:2::2/64 GE0/1 2001:16:4::2/64 D: GE0/3 2001:16:3::2/64 GE0/1 2001:16:5::1/64
Configuration Steps	● Enable IPv6 on interfaces of all routers.(Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router A, configure route filtering.
A	A#configure terminal A(config)#ipv6 access-list test A (config-ipv6-acl)#permit ipv6 2001:16:5::/64 any A(config)#ipv6 router ospf 1 A(config-router)#distribute-list test in GigabitEthernet0/1
Verification	● On Router A, check the routing table. Verify that only the entry 2001:16:5::/64 is loaded.
	O IA 2001:16:5::/64 [110/2] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/1

Common Errors

- Filtering routes by using the **distribute-list in** command affects forwarding of local routes, but does not affect route computation based on LSAs. Therefore, if route filtering is configured on the ABR, Type 3 LSAs will still be generated and advertised to other areas because routes can still be computed based on LSAs. As a result, black-hole routes are generated.

6.4.7 Modifying the Route Cost and AD

Configuration Effect

- Change the OSPF routes so that the traffic passes through specified nodes or bypasses specified nodes.
- Change the sequence that a router selects routes so as to change the priorities of OSPF routes.

Notes

- The OSPF basic functions must be configured.
- If you run the **ipv6 ospf cost** command to configure the cost of an interface, the configured cost will automatically overwrite the cost that is computed based on the auto cost.

Configuration Steps

Configuring the Reference Bandwidth

- Optional.
- A router is connected with lines with different bandwidths. This configuration is recommended if you wish to preferentially select the line with a larger bandwidth.

Configuring the Cost of an Interface

- Optional.
- A router is connected with multiple lines. This configuration is recommended if you wish to manually specify a preferential line.

Configuring the Default Metric for Redistribution

- Optional.
- This configuration is mandatory if the cost of external routes of the OSPF domain should be specified when external routes are introduced to an ASBR.

Configuring the Maximum Metric

- Optional.
- A router may be unstable during the restart process or a period of time after the router is restarted, and users do not want to forward data through this router. In this case, this configuration is recommended.

Configuring the AD

- Optional.
- Perform this configuration if you wish to change the priorities of OSPF routes on a router that runs multiple unicast routing protocols.

Verification

- Run the **show ipv6 ospf interface** command to verify that the costs of interfaces are correct.
- Run the **show ipv6 route** command to verify that the costs of external routes introduced by the ASBR are correct.
- Restart the router. Within a specified period of time, data is not forwarded through the restarted router.

Related Commands

Configuring the Reference Bandwidth

Command	**auto-cost reference-bandwidth** *ref-bw*
Parameter Description	*ref-bw*: Indicates the reference bandwidth. The unit is Mbps. The value ranges from 1 to 4,294,967.
Command Mode	OSPF routing process configuration mode
Usage Guide	You can run the **ipv6 ospf cost** command in interface configuration mode to specify the cost of the interface. The priority of this cost is higher than that of the metric computed based on the reference bandwidth.

Configuring the Cost of an Interface

Command	**ipv6 ospf cost** *cost*[**instance***instance-id*]
Parameter Description	*cost*: Indicates the cost of an OSPF interface. The value ranges from 0 to 65,535. **instance***instance-id:* Indicates the ID of a specified OSPFv3 process of the interface. The value ranges from 0 to 255.
Command Mode	Interface configuration mode
Usage Guide	By default, the cost of an OSPFv3 interface is equal to 100 Mbps/Bandwidth, where Bandwidth is the bandwidth of the interface and configured by the **bandwidth** command in interface configuration mode. The costs of OSPF interfaces on several typical lines are as follows: ● 64 Kbps serial line: The cost is 1562. ● E1 line: The cost is 48. ● 10M Ethernet: The cost is 10. ● 100M Ethernet: The cost is 1. If you run the **ipv6 ospf cost** command to configure the cost of an interface, the configured cost will automatically overwrite the cost that is computed based on the auto cost.

Configuring the Cost of the Default Route in a Stub or an NSSA Area

Command	**area***area-id* **default-cost***cost*
Parameter Description	*area-id*: Indicates the ID of the stub or NSSA area. *cost*: Indicates the cost of the default summarized route injected to the stub or NSSA area. The value ranges from 0 to 16,777,215.
Command Mode	OSPF routing process configuration mode
Usage Guide	This command takes effect only on an ABR in a stub area or an ABR/ASBR in an NSSA area.

Configuring the Default Metric for Redistribution

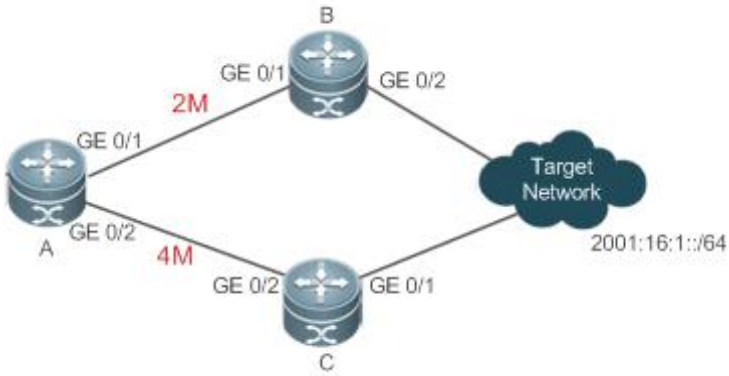
Command	**default-metric** *metric*
Parameter Description	*metric*: Indicates the default metric of the OSPF redistributed route. The value ranges from 1 to 16,777,214.
Command Mode	OSPF routing process configuration mode
Usage Guide	The **default-metric** command must be used together with the **redistribute** command to modify the initial metrics of all redistributed routes. The **default-metric** command does not take effect on external routes that are injected to the OSPF routing domain by the **default-information originate** command. The default metric of a redistributed direct route is always 20.

Configuring the AD

Command	**distance** { *distance* | **ospf**{ [**intra-area***distance*] [**inter-area***distance*] [**external** *distance*]} }
Parameter Description	*distance*: Indicates the AD of a route. The value ranges from 1 to 255. **intra-area***distance*: Indicates the AD of an intra-area route. The value ranges from 1 to 255. **inter-area** *distance*: Indicates the AD of an inter-area route. The value ranges from 1 to 255. **external** *distance:* Indicates the AD of an external route. The value ranges from 1 to 255.
Command Mode	OSPF routing process configuration mode

Usage Guide	Use this command to specify different ADs for different types of OSPF routes. The AD allows different routing protocols to compare route priorities. A smaller AD indicates a higher route priority. The priorities of routes generated by different OSPFv3 processes must be compared based on ADs. If the AD of a route entry is set to 255, the route entry is not trustworthy and does not participate in packet forwarding.

Configuration Example

Scenario	
Configuration Steps	● Enable IPv6 on interfaces of all routers.(Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router A, configure the cost of each interface.
A	A#configure terminal A(config)#interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#ipv6 ospf cost 10 A(config)#interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)#ipv6 ospf cost 20
Verification	● On Router A, check the routing table. The next hop of the optimum path to 2001:16:1::/64 is Router B.
A	A#show ipv6 route ospf IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area O E2 2001:16:1::/64 [110/2] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/1

Common Errors

- If the cost of an interface is set to 0 in the **ipv6 ospf cost** command, a route computation error may occur. For example, a routing loop is obtained.

6.4.8 Enabling Authentication

Configuration Effect

- All routers connected to the OSPF network must be authenticated to ensure stability of OSPF and protect OSPF against intrusions.

Notes

- The OSPF basic functions must be configured.
- If authentication is configured for an area, the configuration takes effect on all interfaces that belong to this area.
- If authentication is configured for both an interface and the area to which the interface belongs, the configuration for the interface takes effect preferentially.

Configuration Steps

Configuring Authentication

- Optional.
- Perform this configuration if a router accesses a network that requires authentication.

Configuring Encryption

- Optional.
- Perform this configuration if a router accesses a network that requires encryption.

Configuring Virtual Link Authentication

- Optional.
- Perform this configuration if a router accesses a network that requires authentication.

Configuring Virtual Link Encryption

- Optional.
- Perform this configuration if a router accesses a network that requires encryption.

Verification

- If routers are configured with different authentication keys, run the **show ipv6 ospf neighbor** command to verify that there is no OSPF neighbor.
- If routers are configured with the same authentication key, run the **show ipv6 ospf neighbor** command to verify that there are OSPF neighbors.

Related Commands

Configuring Area-based Authentication

Command	**area***area-id***authenticationipsec spi***spi***[md5 [string-key] |sha1]** [**0 | 7**] *key*

Parameter Description	*area-id*: Indicates the area ID.The value can be an integer or an IPv4 prefix. *spi*: Indicates the SPI. The value ranges from 256 to 4,294,967,295. **md5:** Enables MD5 authentication. **string-key**: Indicates that MD5 authentication key supports special characters. **sha1:** Enables SHA1 authentication. **0:** Indicates that the key is displayed in plain text. **7:** Indicates that the key is displayed in cipher text. *key:* Indicates the authentication key.
Command Mode	OSPF routing process configuration mode
Usage Guide	The FSOS supports three authentication types: ● No authentication ● MD5 authentication ● SHA1 authentication Configuration of area-based authentication for OSPFv3 takes effect on all interfaces (except virtual links) in the area, but the interface-based authentication configuration takes precedence over the area-based configuration.

Configuring Area-based Encryption and Authentication

Command	**area***area-id***encryption ipsec spi***spi* **esp**[**null**|[**des** | **3des**][**0** | **7**] *des-key*][**md5**|**sha1**] [**0**|**7**] *key*
Parameter Description	*area-id*: Indicates the area ID.The value can be an integer or an IPv4 prefix. *spi*: Indicates the SPI. The value ranges from 256 to 4,294,967,295. **null:** Indicates that no encryption mode is used. **des:** Indicates that the Data Encryption Standard (DES) mode is used. **3des:** Indicates that the Triple DES (3DES) mode is used. des-key: Indicates the encryption key. **md5**: Enables MD5 authentication. **sha1**: Enables SHA1 authentication. **0**: Indicates that the key is displayed in plain text. **7**: Indicates that the key is displayed in cipher text. key: Indicates the authentication key.
Command Mode	OSPF routing process configuration mode
Usage Guide	The FSOS supports two encryption modes and two authentication modes. The two encryption modes are as follows: ● DES ● 3DES The two authentication modes are as follows: ● MD5 ● SHA1 Configuration of area-based encryption and authentication for OSPFv3 takes effect on all interfaces (except virtual links) in the area, but the interface-based encryption and authentication configuration takes precedence over the area-based configuration.

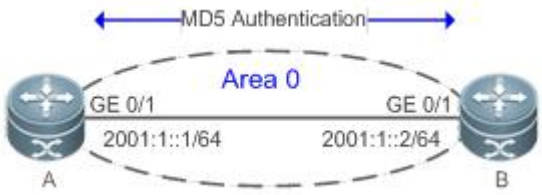
Configuring Interface-based Authentication

Command	**ipv6 ospfauthentication**[**null** | **ipsec spi***spi*[**md5 [string-key]**|**sha1**] [**0**|**7**]*key*][**instance***instance-id*]
Parameter Description	*area-id*: Indicates the area ID.The value can be an integer or an IPv4 prefix. *spi*: Indicates the SPI. The value ranges from 256 to 4,294,967,295. **md5:** Enables MD5 authentication. **string-key**: Indicates that MD5 authentication key supports special characters. **sha1:** Enables SHA1 authentication. **0:** Indicates that the key is displayed in plain text. **7:** Indicates that the key is displayed in cipher text. *key:* Indicates the authentication key. **instance** *instance-id:* Indicates the ID of a specified OSPFv3 process of the interface. The value ranges from 0 to 255.
Command Mode	OSPF routing process configuration mode
Usage Guide	The FSOS supports three authentication types: ● No authentication ● MD5 authentication ● SHA1 authentication OSPFv3 authentication parameters configured on interconnected interfaces must be consistent.

Configuring Interface-based Encryption and Authentication

Command	**ipv6 ospfencryption ipsec spi***spi* **esp**[**null**|[**des** | **3des**][**0** | **7**] *des-key*][**md5**|**sha1**] [**0**|**7**] *key*[**instance***instance-id*]
Parameter Description	*spi*: Indicates the SPI. The value ranges from 256 to 4,294,967,295. **null:** Indicates that no encryption mode is used. **des:** Indicates that the DES mode is used. **3des:** Indicates that the3DES mode is used. des-key: Indicates the encryption key. **md5**: Enables MD5 authentication. **sha1**: Enables SHA1 authentication. **0**: Indicates that the key is displayed in plain text. **7**: Indicates that the key is displayed in cipher text. key: Indicates the authentication key. **instance** *instance-id:* Indicates the ID of a specified OSPFv3 process of the interface. The value ranges from 0 to 255.
Command Mode	OSPF routing process configuration mode
Usage Guide	The FSOS supports two encryption modes and two authentication modes. The two encryption modes are as follows: ● DES ● 3DES The two authentication modes are as follows: ● MD5 ● SHA1 OSPFv3 encryption and authentication parameters configured on the local interface must be consistent with those configured on the interconnected interfaces.

Configuration Example

Scenario	
Configuration Steps	● Enable IPv6 on interfaces of all routers.(Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Configure MD5 authentication for interfaces of all routers.
A	A#configure terminal A(config)#interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#ipv6 ospf authentication ipsec spi 256 md5 01234567890123456789012345678912
B	B# configure terminal B(config)#interface GigabitEthernet 0/3 B(config-if-GigabitEthernet 0/3)#ipv6 ospf authentication ipsec spi 256 md5 01234567890123456789012345678912
Verification	● On Router A and Router B, verify that the OSPF neighbor status is correct.
A	A# show ipv6 ospf neighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Instance ID Interface 2.2.2.2 1 Full/DR 00:00:38 0 GigabitEthernet 0/1
B	B# show ipv6 ospf neighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Instance ID Interface 1.1.1.1 1 Full/BDR 00:00:38 0 GigabitEthernet 0/1

Common Errors

- The configured authentication modes are inconsistent.
- The configured authentication keys are inconsistent.

6.4.9 Modifying the Maximum Number of Concurrent Neighbors

Configuration Effect

- Control the maximum number of concurrent neighbors on the OSPF process to ease the pressure on the device.

Notes

- The OSPF basic functions must be configured.

Configuration Steps

Configuring the Maximum Number of Concurrent Neighbors on the OSPF Process

- (Optional) This configuration is recommended if you wish to set up the OSPF adjacency more quickly when a router is connected with a lot of other routers.
- Perform this configuration on a core router.

Verification

- Run the **show ipv6 ospf neighbor** command to display the number of neighbors that are concurrently interacting with the OSPF process.

Related Commands

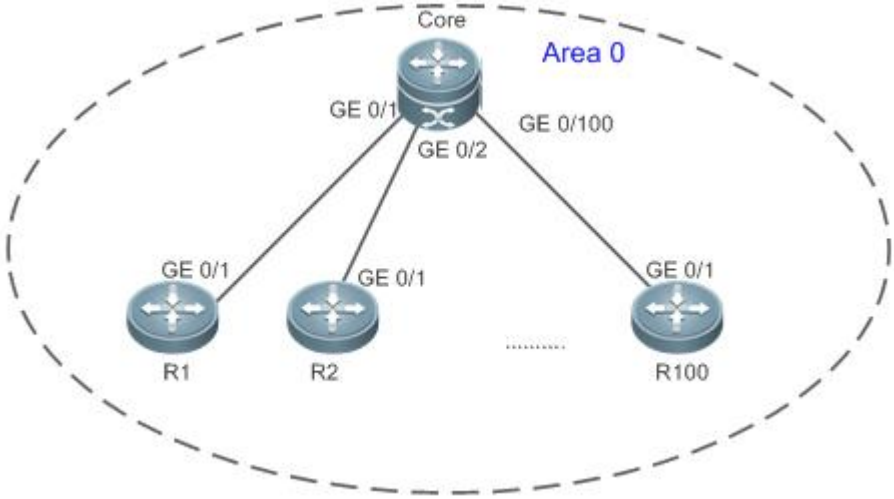
Configuring the Maximum Number of Concurrent Neighbors on the Current Process

Command	**max-concurrent-dd***number*
Parameter Description	*number:* Specifies the maximum number of neighbors that are concurrently interacting with the OSPF process. The value ranges from 1 to 65,535.
Command Mode	OSPF routing process configuration mode
Usage Guide	When the performance of a router is affected because the router exchanges data with multiple neighbors, you can configure this command to restrict the maximum of neighbors with which each OSPF process can concurrently initiate or accept interaction.

Configuring the Maximum Number of Concurrent Neighbors on All Processes

Command	**Ipv6 router ospf max-concurrent-dd***number*
Parameter Description	*number:* Specifies the maximum number of neighbors that are concurrently interacting with the OSPF process. The value ranges from 1 to 65,535.
Command Mode	Global configuration mode
Usage Guide	When the performance of a router is affected because the router exchanges data with multiple neighbors, you can configure this command to restrict the maximum of neighbors with which all OSPF processes can concurrently initiate or accept interaction.

Configuration Example

Scenario	
Configuration Steps	● Enable IPv6 on interfaces of all routers.(Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On the Router Core, set the maximum number of concurrent neighbors to 4.
Core	Core# configure terminal Core(config)# ipv6 router ospf max-concurrent-dd 4
Verification	● On the Router Core, check the neighbor status and verify that at most eight neighbors concurrently interact with the OSPF process.

Common Errors

N/A

6.4.10 Disabling MTU Verification

Configuration Effect

- The unicast routing service can be provided even if the MTUs of interfaces on neighbor routers are different.

Notes

- The OSPF basic functions must be configured.

Configuration Steps

Disabling MTU Verification

- (Optional) MTU verification is disabled by default. You are advised to retain the default configuration.
- Perform this configuration on two routers with different interface MTUs.

Verification

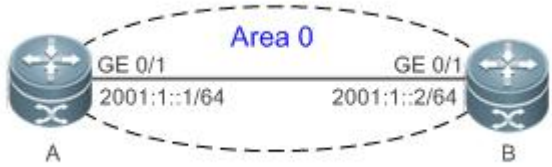
- The adjacency can be set up between routers with different MTUs.

Related Commands

Disabling MTU Verification

Command	**Ipv6 ospf mtu-ignore**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	On receiving the database description packet, OSPF checks whether the MTU of the interface on the neighbor is the same as the MTU of its own interface. If the interface MTU specified in the received database description packet is greater than the MTU of the local interface, the adjacency cannot be set up. To resolve this problem, you can disable MTU verification.

Configuration Example

Scenario	
Configuration Steps	● Enable IPv6 on interfaces of all routers.(Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Configure different MTUs for interfaces on two routers. ● Disable MTU verification on all routers. (By default, the function of disabling MTU verification is enabled.)
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ipv6 mtu 1400 A(config-if-GigabitEthernet 0/1)#ipv6 ospf mtu-ignore
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ipv6 mtu 1600 B(config-if-GigabitEthernet 0/1)# ipv6 ospf mtu-ignore
Verification	● On Router A, verify that the OSPF neighbor information is correct.
A	A# show ipv6 ospf neighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Instance ID Interface 2.2.2.2 1 Full/DR 00:00:38 0 GigabitEthernet 0/1

Common Errors

N/A

6.4.11 Enabling Two-Way Maintenance

Configuration Effect

- Non-Hello packets can also be used to maintain the adjacency.

Notes

- The OSPF basic functions must be configured.

Configuration Steps

Enabling Two-Way Maintenance

- (Optional) This function is enabled by default. You are advised to retain the default configuration.
- Perform this configuration on all routers.

Verification

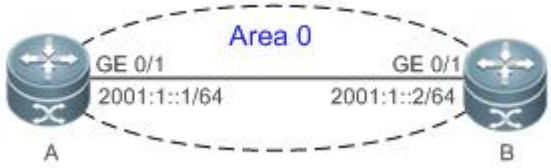
- Non-Hello packets can also be used to maintain the adjacency.

Related Commands

Enabling Two-Way Maintenance

Command	two-way-maintain
Parameter Description	N/A
Command Mode	OSPF routing process configuration mode
Usage Guide	On a large network, a lot of packets may be sent or received, occupying too much CPU and memory. As a result, some packets are delayed or discarded. If the processing time of Hello packets exceeds the dead interval, the adjacency will be destroyed due to timeout.If the two-way maintenance function is enabled, in addition to the Hello packets, the DD, LSU, LSR, and LSAck packets can also be used to maintain the bidirectional communication between neighbors when a large number of packets exist on the network. This prevents termination of the adjacency caused by delayed or discarded Hello packets.

Configuration Example

Scenario	
Configuration Steps	• Enable IPv6 on interfaces of all routers.(Omitted) • Configure the OSPF basic functions on all routers. (Omitted) • On Router A, enable the two-way maintenance function. (This function is enabled by default.)

A	A# configure terminal A(config)# ipv6 routerospf 1 A(config-router)#two-way-maintain
Verification	● When the adjacency is being set up, Router A checks the neighbor dead interval and updates the dead interval without waiting for Router B to send a Hello packet.
A	A# show ipv6 ospfneighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Instance ID Interface 2.2.2.2 1 Full/DR 00:00:38 0 GigabitEthernet 0/1

Common Errors

N/A

6.4.12 Enabling GR

Configuration Effect

- When a distributed route switches services from the active board to the standby board, traffic forwarding continues and is not interrupted.
- When the OSPF process is being restarted, data forwarding continues and is not interrupted.

Notes

- The OSPF basic functions must be configured.
- The neighbor router must support the GR helper function.
- The grace period cannot be shorter than the neighbor dead time of the neighbor router.

Configuration Steps

Configuring the OSPF GR Function

- (Optional) This function is enabled by default. You are advised to retain the default configuration.
- Perform this configuration on routers where hot standby switchover is triggered or the OSPF process is restarted.

Configuring the OSPF GR Helper Function

- (Optional) This function is enabled by default. You are advised to retain the default configuration.
- Perform this configuration on a router if hot standby switchover is triggered or the OSPF process is restarted on a neighbor of this router.

Verification

- When a distributed router switches services from the active board to the standby board, data forwarding continues and the traffic is not interrupted.
- When the OSPF process is being restarted, data forwarding continues and the traffic is not interrupted.

Related Commands

Configuring the OSPF GR Function

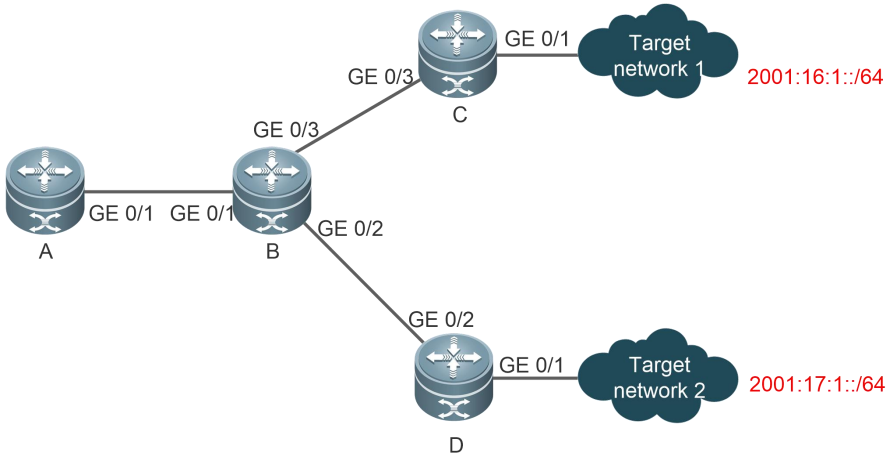
Command	**graceful-restart** [**grace-period***grace-period*|**inconsistent-lsa-checking**]
Parameter Description	**grace-period** *grace-period*: Indicates the grace period, which is the maximum time from occurrence of an OSPF failure to completion of the OSPF GR. The value of the grace period varies from 1s to 1800s. The default value is 120s. **inconsistent-lsa-checking**: Enables topological change detection. If any topological change is detected, OSPF exits the GR process to complete convergence.After GR is enabled, topological change detection is enabled by default.
Command Mode	OSPF routing process configuration mode
Usage Guide	The GR function is configured based on the OSPF process. You can configure different parameters for different OSPF processes based on the actual conditions. This command is used to configure the GR restarter capability of a device. The grace period is the maximum time of the entire GR process, during which link status is rebuilt so that the original state of the OSPF process is restored. After the grace period expires, OSPF exits the GR state and performs common OSPF operations. Run the **graceful-restart** command to set the grace period to 120s. The **graceful-restart grace-period** command allows you to modify the grace period explicitly. The precondition for successful execution of GR and uninterrupted forwarding is that the topology remains stable. If the topology changes, OSPF quickly converges without waiting for further execution of GR, thus avoiding long-time forwarding black-hole. ● Disabling topology detection: If OSPF cannot converge in time when the topology changes during the hot standby process, forwarding black-hole may appear in a long time. ● Enabling topology detection: Forwarding may be interrupted when topology detection is enabled, but the interruption time is far shorter than that when topology detection is disabled. In most cases, it is recommended that topology detection be enabled. In special scenarios, topology detection can be disabled if the topology changes after the hot standby process, but it can be ensured that the forwarding black-hole will not appear in a long time. This can minimize the forwarding interruption time during the hot standby process. If the Fast Hello function is enabled, the GR function cannot be enabled.

Configuring the OSPF GR Helper Function

Command	**graceful-restart helper** { **disable** |**strict-lsa-checking** | **internal-lsa-checking**}
Parameter Description	**disable**: Prohibits a device from acting as a GR helper for another device. **strict-lsa-checking**: Indicates that changes in Type 1 to Type 5 and Type 7 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network changes, the device will stop acting as the GR helper. **internal-lsa-checking:** Indicates that changes in Type 1 to Type 3 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network changes, the device will stop acting as the GR helper.
Command Mode	OSPF routing process configuration mode
Usage Guide	This command is used to configure the GR helper capability of a router. When a neighbor router implements GR, it sends a Grace-LSA to notify all neighbor routers. If the GR helper function is enabled on the local router, the local router becomes the GR helper on receiving the Grace-LSA, and helps the neighbor to complete GR. The **disable** option indicates that GR helper is not provided for any device that implements GR.

	After a device becomes the GR helper, the network changes are not detected by default. If any change takes place on the network, the network topology converges after GR is completed. If you wish that network changes can be quickly detected during the GR process, you can configure **strict-lsa-checking** to check Type 1 to 5 and Type 7 LSAs that indicate the network information or **internal-lsa-checking** to check Type 1 to 3 LSAs that indicate internal routes of the AS domain. When the network scale is large, it is recommended that you disable the LSA checking options (**strict-lsa-checking** and **internal-lsa-checking**) because regional network changes may trigger termination of GR and consequently reduce the convergence of the entire network.

Configuration Example

Scenario	
Configuration Steps	• Enable IPv6 on interfaces of all routers.(Omitted) • Configure the OSPF basic functions on all routers. (Omitted) • On Router A, Router C, and Router D, enable the GR helper function. (This function is enabled by default.) • On Router B, enable the GR function.
B	B# configure terminal B(config)# ipv6 router ospf1 B(config-router)# graceful-restart
Verification	• Trigger a hot standby switchover on Router B, and verify that the routing tables of destination Network 1 and Network 2 remain unchanged on Router A during the switchover. • Trigger a hot standby switchover on Router B, ping destination Network 1 from Router A, and verify that traffic forwarding is not interrupted during the switchover.

Common Errors

- Traffic forwarding is interrupted during the GR process because the configured grace period is shorter than the neighbor dead time of the neighbor router.

6.4.13 Configuring Network Management Functions

Configuration Effect

- Use the network management software to manage OSPF parameters and monitor the OSPF running status.

Notes

- The OSPF basic functions must be configured.
- You must enable the MIB function of the SNMP server before enabling the OSPF MIB function.
- You must enable the trap function of the SNMP server before enabling the OSPF trap function.
- You must enable the logging function of the device before outputting the OSPF logs.

Configuration Steps

Binding the MIB with the OSPF Process

- (Optional) This configuration is required if you want to use the network management software to manage parameters of a specified OSPF process.
- Perform this configuration on all routers.

Enabling the Trap Function

- (Optional) This configuration is required if you want to use the network management software to monitor the OSPF running status.
- Perform this configuration on all routers.

Configuring the Logging Function

- (Optional) This function is enabled by default. You are advised to retain the default configuration. If you want to reduce the log output, disable this function.
- Perform this configuration on all routers.

Verification

- Use the network management software to manage the OSPF parameters.
- Use the network management software to monitor the OSPF running status.

Related Commands

Binding the MIB with the OSPF Process

Command	**enable mib-binding**
Parameter Description	N/A
Command Mode	OSPF routing process configuration mode
Usage Guide	The OSPFv2 MIB does not have the OSPFv3 process information. Therefore, you can perform operations only on a single OSPFv2 process through SNMP. By default, the OSPFv3 MIB is bound with the OSPFv3 process with the smallest process ID, and all user operations take effect on this process. If you wish to perform operations on a specified OSPFv3 process through SNMP, run this command to bind the MIB with the process.

Enabling the Trap Function

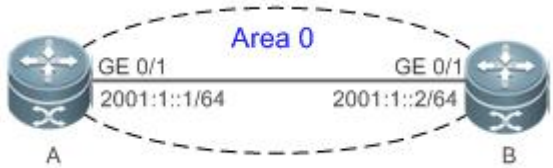
Command	**enable traps**[**error** [**IfConfigError**| **IfRxBadPacket** | **VirtIfConfigError** | **VirtIfRxBadPacket**] | **state-change**[**IfStateChange** | **NbrStateChange** | **NssaTranslatorStatusChange** | **VirtIfStateChange** | **VirtNbrStateChange** | **RestartStatusChange** |

	NbrRestartHelperStatusChange | VirtNbrRestartHelperStatusChange]]
Parameter Description	**IfConfigError:** Indicates that an interface parameter configuration error occurs. **IfRxBadPacket:** Indicates that the interface receives a bad packet. **VirtIfConfigError:** Indicates that a virtual interface parameter configuration error occurs. **VirtIfRxBadPacket:** Indicates that the virtual interface receives a bad packet. **IfStateChange:** Indicates that interface state changes. **NbrStateChange:** Indicates that the neighbor state changes. **NssaTranslatorStatusChange:** Indicates that the NSSA translation state changes. **VirtIfStateChange:** Indicates that the virtual interface state changes. **VirtNbrStateChange:** Indicates that the virtual neighbor state changes. **RestartStatusChange:** Indicates that the GR state of the local device changes. **NbrRestartHelperStatusChange:** Indicates that the state of the neighbor GR process changes. **VirtNbrRestartHelperStatusChange:** Indicates that the GR state of the virtual neighbor changes.
Command Mode	OSPF routing process configuration mode
Usage Guide	The function configured by this command is restricted by the **snmp-server** command. You can configure **snmp-server enable traps ospf** and then **enable traps** command before the corresponding OSPF traps can be correctly sent out. This command is not restricted by the MIB bound with the process. The trap function can be enabled concurrently for different processes.

Configuring the Logging Function

Command	**log-adj-changes**[**detail**]
Parameter Description	**detail**: Records all status change information.
Command Mode	OSPF routing process configuration mode
Usage Guide	N/A

Configuration Example

Scenario	
Configuration Steps	● Enable IPv6 on interfaces of all routers.(Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Bind the MIB with the OSPF process on Router A. ● Enable the trap function on Router A.

A	A# configure terminal A(config)#snmp-server host 192.168.2.2 traps version 2c public A(config)#snmp-server community public rw A(config)#snmp-server enable traps A(config)# A(config)# ipv6 routerospf 10 A(config-router)# enable mib-binding A(config-router)# enable traps
Verification	● Use the MIB tool to read and set the OSPF parameters and display the OSPF running status.

Common Errors

N/A

6.4.14 Modifying Protocol Control Parameters

Configuration Effect

- Modify protocol control parameters to change the protocol running status.

Notes

- The OSPF basic functions must be configured.
- The neighbor dead time cannot be shorter than the Hello interval.

Configuration Steps

Configuring the Hello Interval

- (Optional) You are advised to retain the default configuration.
- Perform this configuration on routers at both end of a link.

Configuring the Dead Interval

- (Optional) You are advised to retain the default configuration. This configuration can be adjusted if you wish to accelerate OSPF convergence when a link fails.
- Perform this configuration on routers at both end of a link.

Configuring the LSU Retransmission Interval

- (Optional) You are advised to adjust this configuration if a lot of routes exist in the user environment and network congestion is serious.

Configuring the LSA Generation Time

- (Optional) You are advised to retain the default configuration.

Configuring the LSA Group Refresh Time

- (Optional) You are advised to retain the default configuration. This configuration can be adjusted if a lot of routes exist in the user environment.
- Perform this configuration on an ASBR or ABR.

Configuring LSA Repeated Receiving Delay

- (Optional) You are advised to retain the default configuration.

Configuring the SPF Computation Delay

- (Optional) This configuration can be adjusted if network flapping frequently occurs.

Configuring the Inter-Area Route Computation Delay

- (Optional) You are advised to retain the default configuration.
- Perform this configuration on all routers.

Configuring the Inter-Area Route Computation Delay

- (Optional) You are advised to retain the default configuration.
- Perform this configuration on all routers.

Verification

- Run the **show ipv6 ospf** and **show ipv6 ospf neighbor** commands to display the protocol running parameters and status.

Related Commands

Configuring the Hello Interval

Command	**ipv6ospf hello-interval***seconds*
Parameter Description	*seconds*: Indicates the interval at which OSPF sends the Hello packet. The unit is second. The value ranges from 1 to 65,535.
Command Mode	Interface configuration mode
Usage Guide	The Hello interval is contained in the Hello packet. A shorter Hello interval indicates that OSPF can detect topological changes more quickly, but the network traffic increases. The Hello interval must be the same on all routers in the same network segment. If you want to manually modify the neighbor dead interval, ensure that the neighbor dead interval is longer than the Hello interval.

Configuring the Dead Interval

Command	**ipv6ospf dead-interval** *seconds*
Parameter Description	*seconds*: Indicates the time that the neighbor is declared lost. The unit is second. The value ranges from 1 to 65,535.
Command Mode	Interface configuration mode
Usage Guide	The OSPF dead interval is contained in the Hello packet. If OSPF does not receive a Hello packet from a neighbor within the dead interval, it declares that the neighbor is invalid and deletes this neighbor record form the neighbor list. By default, the dead interval is four times the Hello interval. If the Hello interval is modified, the dead interval is modified

	automatically. When using this command to manually modify the dead interval, pay attention to the following issues: 1. The dead interval cannot be shorter than the Hello interval. 2. The dead interval must be the same on all routers in the same network segment.

Configuring the LSU Transmission Delay

Command	**ipv6ospf transmit-delay***seconds*
Parameter Description	*seconds*: Indicates the LSU transmission delay on the OSPF interface. The unit is second. The value ranges from 0 to 65,535.
Command Mode	Interface configuration mode
Usage Guide	Before an LSU packet is transmitted, the Age fields in all LSAs in this packet will increase based on the amount specified by the **ip ospf transmit-delay** command. Considering the transmission delay and line propagation delay on the interface, you need to set the LSU transmission delay to a greater value for a low-speed line or interface. The LSU transmission delay of a virtual link is defined by the **transmit-delay** parameter in the **area virtual-link** command. If the value of the Age field of an LSA reaches 3600, the packet will be retransmitted or a retransmission will be requested. If the LSA is not updated in time, the expired LSA will be deleted from the LSDB.

Configuring the LSU Retransmission Interval

Command	**ipv6ospf retransmit-interval***seconds*
Parameter Description	*seconds*: Indicates the LSU retransmission interval. The unit is second. The value ranges from 0 to 65,535. This interval must be longer than the round-trip transmission delay of data packets between two neighbors.
Command Mode	Interface configuration mode
Usage Guide	After a router finishes sending an LSU packet, this packet is still kept in the transmit buffer queue. If an acknowledgment from the neighbor is not received within the time defined by the **ip ospf retransmit-interval** command, the router retransmits the LSU packet. The retransmission delay can be set to a greater value on a serial line or virtual link to prevent unnecessary retransmission. The LSU retransmission delay of a virtual link is defined by the **retransmit-interval**parameter in the **area virtual-link** command.

Configuring the LSA Generation Time

Command	**timers throttle lsa all** *delay-time hold-time max-wait-time*
Parameter Description	*delay-time*: Indicates the minimum delay for LSA generation. The first LSA in the database is always generated instantly. The value ranges from 0 to 600,000. The unit is ms. *hold-time*: Indicates the minimum interval between the first LSA update and the second LSA update. The value ranges from 1 to 600,000. The unit is ms. *max-wait-time*: Indicates the maximum interval between two LSA updates when the LSA is updated continuously. This interval is also used to determine whether the LSA is updated continuously. The value ranges from 1 to 600,000. The unit is ms.
Command Mode	OSPF routing process configuration mode
Usage Guide	If a high convergence requirement is raised when a link changes, you can set **delay-time** to a smaller value. You can also appropriately increase values of the preceding parameters to reduce the CPU usage.

	When configuring this command, the value of **hold-time** cannot be smaller than the value of **delay-time,** and the value of **max-wait-time** cannot be smaller than the value of **hold-time**.

Configuring the LSA Group Refresh Time

Command	**timers pacinglsa-group** *seconds*
Parameter Description	*seconds*: Indicates the LSA group pacing interval. The value ranges from 10 to 1,800. The unit is second.
Command Mode	OSPF routing process configuration mode
Usage Guide	Every LSA has a time to live (LSA age). When the LSA age reaches 1800s, a refreshment is needed to prevent LSAs from being cleared because their ages reaching the maximum. If LSA update and aging computation are performed for every LSA, the device will consume a lot of CPU resources. In order to use CPU resources effectively, you can refresh LSAs by group on the device. The interval of group refreshment is called group pacing interval. The group refreshment operation is to organize the LSAs generated within a group pacing interval into a group and refresh the group as a whole. If the total number of LSAs does not change, a larger group pacing interval indicates that more LSAs need to be processed after timeout. To maintain the CPU stability, the number of LSAs processes upon each timeout cannot be too large. If the number of LSAs is large, you are advised to reduce the group pacing interval. For example, if there are 1000 LSAs in the database, you can reduce the pacing interval; if there are 40 to 100 LSAs, you can set the pacing interval to 10-20 minutes.

Configuring the LSA Group Refresh Interval

Command	**timers pacing lsa-transmit** *transmit-time transmit-count*
Parameter Description	*transmit-time*: Indicates the LSA group transmission interval. The value ranges from 10 to 600,000. The unit is ms. *transmit-count*: Indicates the number of LS-UPD packets in a group. The value ranges from 1 to 200.
Command Mode	OSPF routing process configuration mode
Usage Guide	If the number of LSAs is large and the device load is heavy in an environment, properly configuring **transimit-time** and **transimit-count** can limit the number of LS-UPD packets flooded on a network. If the CPU usage is not high and the network bandwidth load is not heavy, reducing the value of **transimit-time** and increasing the value of **transimit-count** can accelerate the environment convergence.

Configuring LSA Repeated Receiving Delay

Command	**timers lsa arrival***arrival-time*
Parameter Description	*arrival-time*: Indicates the delay after which the same LSA is received. The value ranges from 0 to 600,000. The unit is ms.
Command Mode	OSPF routing process configuration mode
Usage Guide	No processing is performed if the same LSA is received within the specified time.

Configuring the SPF Computation Delay

Command	**timers throttle spf** *spf-delay spf-holdtime spf-max-waittime*
Parameter Description	*spf-delay*: Indicates the SPF computation delay. The unit is ms. The value ranges from 1 to 600,000. When detecting a topological change, the OSPF routing process triggers the SPF computation at least after **spf-delay** elapses.

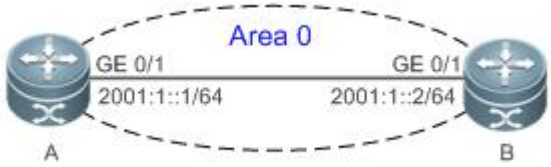
	spf-holdtime: Indicates the minimum interval between two SPF computations. The unit is ms. The value ranges from 1 to 600,000. *spf-max-waittime*: Indicates the maximum interval between two SPF computations. The unit is ms. The value ranges from 1 to 600,000. *number*: Indicates the metric of the summarized route.
Command Mode	OSPF routing process configuration mode
Usage Guide	**spf-delay** indicates the minimum time between the occurrence of the topological change and the start of SPF computation. **spf-holdtime** indicates the minimum interval between the first SPF computation and the second SPF computation. After that, the interval between two SPF computations must be at least twice of the previous interval. When the interval reaches **spf-max-waittime**, the interval cannot increase again. If the interval between two SPF computations already exceeds the required minimum value, the interval is computed by starting from **spf-holdtime**. You can set **spf-delay** and **spf-holdtime** to smaller values to accelerate topology convergence, and set **spf-max-waittime** to a larger value to reduce SPF computation. Flexible settings can be used based on stability of the network topology. Compared with the **timers spf** command, this command supports more flexible settings to accelerate the convergence speed of SPF computation and further reduce the system resources consumed by SPF computation when the topology continuously changes. Therefore, you are advised to use the **timers throttle spf** command for configuration. 1. The value of **spf-holdtime** cannot be smaller than the value of **spf-delay**; otherwise, **spf-holdtime** will be automatically set to the value of **spf-delay**. 2. The value of **spf-max-waittime** cannot be smaller than the value of **spf-holdtime**; otherwise, **spf-max-waittime** will be automatically set to the value of **spf-holdtime**. 3. The configurations of **timers throttle spf** and **timers spf** are mutually overwritten. 4. When both **timers throttle spf** and **timers spf** are not configured, the default values of **timers throttle spf** prevail.

Configuring the Computation Delays of Inter-Area Routes and External Routes

Command	**timers throttle route**{**inter-area***ia-delay*|**ase***ase-delay*}
Parameter Description	**inter-area***ia-delay*: Indicates the inter-area route computation delay. The unit is ms. The value ranges from 0 to 600,000. **ase***ase-delay:* Indicates the external route computation delay. The unit is ms. The value ranges from 0 to 600,000.
Command Mode	OSPF routing process configuration mode
Usage Guide	If a strict requirement is raised for the network convergence time, use the default value. If a lot of inter-area or external routes exist on the network and the network is not stable, adjust the delays and optimize route computation to reduce the load on the device.

Configuration Example

Configuring the Hello Interval and Dead Interval

Scenario	

Configuration Steps	● Enable IPv6 on interfaces of all routers.(Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Configure the Hello interval and dead interval on all routers.
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ipv6 ospf hello-interval 15 A(config-if-GigabitEthernet 0/1)# ipv6 ospf dead-interval 50
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ipv6 ospf hello-interval 15 A(config-if-GigabitEthernet 0/1)# ipv6 ospf dead-interval 50
Verification	● Check the interface parameters on Router A and Router B. Verify that the Hello interval is 10s and the dead interval is 50s. ● On Router A and Router B, verify that the OSPF neighbor information is correct.
A	A# show ipv6 ospf interface GigabitEthernet 0/1 is up, line protocol is up Interface ID 2 IPv6 Prefixes fe80::2d0:f8ff:fe22:3346/64 (Link-Local Address) OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0 Router ID 1.1.1.1,Network Type BROADCAST, Cost: 1 Transmit Delay is 1 sec, State DR, Priority 1 Timer interval configured, Hello 15, Dead 50, Wait 40, Retransmit 10 Hello due in 00:00:06 Neighbor Count is 1, Adjacent neighbor count is 1 Hello received 40 sent 40, DD received 17 sent 9 LS-Req received 1 sent 3, LS-Upd received 6 sent 5 LS-Ack received 3 sent 4, Discarded 1 A# show ipv6 ospf neighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Instance ID Interface 2.2.2.21 Full/BDR 00:00:30 0 GigabitEthernet 0/1

B	B# show ipv6 ospf interface
	GigabitEthernet 0/1 is up, line protocol is up
	  Interface ID 2
	  IPv6 Prefixes
	  fe80::2d0:f8ff:fe22:3446/64 (Link-Local Address)
	  OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0
	  Router ID 2.2.2.2,Network Type BROADCAST, Cost: 1
	  Transmit Delay is 1 sec, State BDR, Priority 1
	  Timer interval configured, Hello 15, Dead 50, Wait 40, Retransmit 10
	  Hello due in 00:00:06
	  Neighbor Count is 1, Adjacent neighbor count is 1
	  Hello received 40 sent 40, DD received 17 sent 9
	  LS-Req received 1 sent 3, LS-Upd received 6 sent 5
	  LS-Ack received 3 sent 4, Discarded 1
	
	B# show ipv6 ospf neighbor
	OSPFv3 Process (1), 1 Neighbors, 1 is Full:
	Neighbor ID Pri State Dead Time Instance ID Interface
	1.1.1.11 Full/DR 00:00:38 0 GigabitEthernet 0/1

Common Errors

- The configured neighbor dead time is shorter than the Hello interval.

6.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears and resets an OSPF process.	**clear ipv6 ospf** [*process-id*]**process**

Displaying

Description	Command
Displays the OSPF process configurations.	**show ipv6 ospf** [*process-id*]
Displays information about the OSPF LSDB.	**show ipv6 ospf**[*process- id*] **database**[*lsa-type* [**adv-router***router-id*]]
Displays OSPF-enabled interfaces.	**show ipv6 ospf** [*process-id*] **interface** [*interface-type interface-number* | **brief**]

Description	Command
Displays the OSPF neighbor list.	**show ipv6 ospf**[*process- id*] **neighbor**[*interface-type interface-number*[**detail**]| *neighbor-id* |**detail**]
Displays the OSPF routing table.	**show ipv6 ospf** [*process-id*] **route**[**count**]
Displays the summarized route of OSPF redistributed routes.	**showipv6ospf**[*process-id*]**summary-prefix**
Displays the OSPF network topology information.	**show ipv6 ospf**[*process- id*] **topology** [**area***area-id*]
Displays OSPF virtual links.	**show ipv6 ospf** [*process-id*] **virtual-links**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs OSPF events.	**debug ipv6 ospf events** [**abr**|**asbr**|**os**|**nssa**|**router**| **vlink**]
Debugs OSPF interfaces.	**debug ipv6 ospf ifsm** [**events**|**status**|**timers**]
Debugs OSPF neighbors.	**debug ipv6 ospf nfsm** [**events** | **status** | **timers**]
Debugs the OSPF NSM.	**debug ipv6 ospf nsm** [**interface** | **redistribute** | **route**]
Debugs OSPF LSAs.	**debug ipv6 ospf lsa** [**flooding** | **generate** | **install** | **maxage** | **refresh**]
Debugs OSPF packets.	**debug ipv6 ospf packet** [**dd**|**detail**|**hello**|**ls-ack**|**ls-request**|**ls-update**|**recv**|**send**]
Debugs OSPF routes.	**debug ipv6 ospf route** [**ase** | **ia** | **install** | **spf** | **time**]

7 Managing Routes

7.1 Overview

The network service module (NSM) manages the routing table, consolidates routes sent by various routing protocols, and selects and sends preferred routes to the routing table. Routes discovered by various routing protocols are stored in the routing table. These routes are generally classified by source into three types:

- Direct route: It is the route discovered by a link-layer protocol and is also called interface route.
- Static route: It is manually configured by the network administrator. A static route is easy to configure and less demanding on the system, and therefore applicable to a small-sized network that is stable and has a simple topology. However, when the network topology changes, the static route must be manually reconfigured and cannot automatically adapt to the topological changes.
- Dynamic route: It is the route discovered by a dynamic routing protocol.

7.2 Applications

Application	Description
Basic Functions of the Static Route	Manually configure a route.
Floating Static Route	Configure a standby route in the multipath scenario.
Load Balancing Static Route	Configure load balancing static routes in the multipath scenario.

7.2.1 Basic Functions of the Static Route

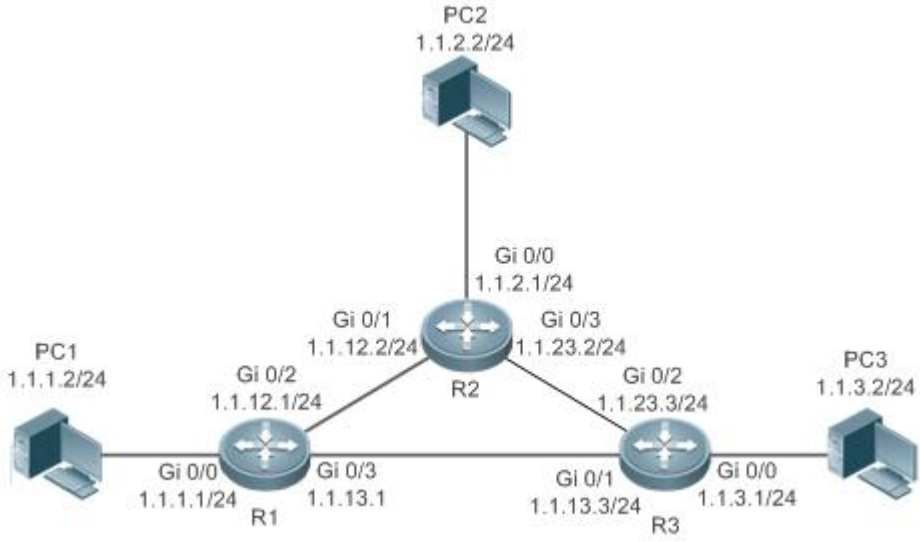
Scenario

On a network with a simple topology, you can configure only static routes to implement network interworking. Appropriate configuration and use of static routes can improve the network performance and guarantee the bandwidth for important network applications.

As shown in Figure 7- 1, to implement interworking between PC 1, PC 2, and PC 3, you can configure static routes on R 1, R 2, and R 3.

- On R 1, configure a route to the network segment of PC 2 through R 2, and a route to the network segment of PC 3 through R 3.
- On R 2, configure a route to the network segment of PC 1 through R 1, and a route to the network segment of PC 3 through R 3.
- On R 3, configure a route to the network segment of PC 1 through R 1, and a route to the network segment of PC 2 through R 2.

Figure 7- 1



Deployment

- Configure the address and subnet mask of each interface.
- Configure static routes on R 1, R 2, and R 3.

7.2.2 Floating Static Route

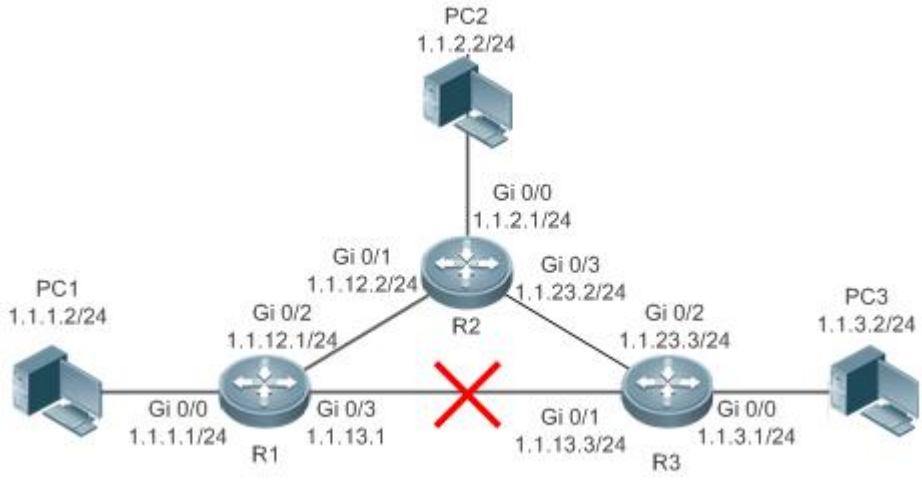
Scenario

If no dynamic routing protocol is configured, you can configure floating static routes to implement dynamic switching of routes to prevent communication interruption caused by the network connection failures.

As shown in Figure 7- 2, to prevent communication interruption caused by a line failure between R 1 and R 3, you can configure a floating static route respectively on R 1 and R 3. Normally, packets are forwarded on a path with a small administrative distance. If a link on this path is down, the route is automatically switched to the path with a large administrative distance.

- On R1, configure two routes to the network segment of PC 3, including a route through R 3 (default distance = 1) and a route through R 2 (default distance = 2).
- On R 3, configure two routes to the network segment of PC 1, including a route through R 1 (default distance = 1) and a route through R 2 (default distance = 2).

Figure 7- 2



Deployment

- Configure the address and subnet mask of each interface.
- Configure static routes on R 1, R 2, and R 3.

7.2.3 Load Balancing Static Route

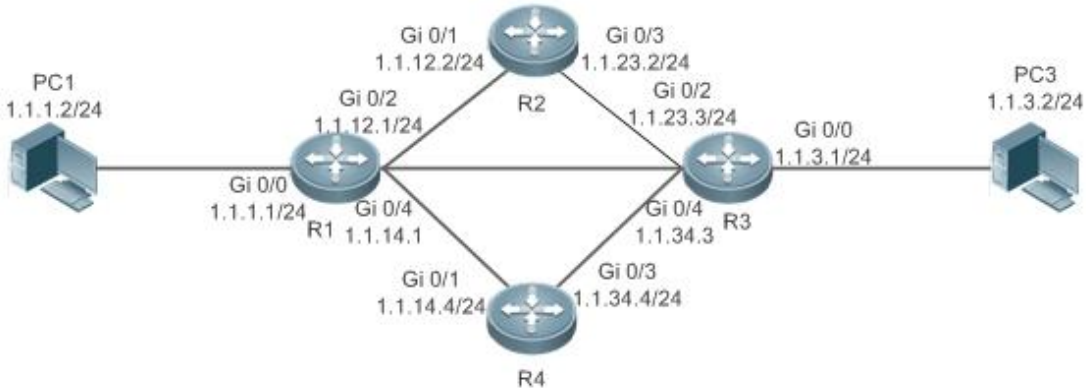
Scenario

If there are multiple paths to the same destination, you can configure load balancing routes. Unlike floating routes, the administrative distances of load balancingroutes are the same. Packets are distributed among these routes based on the balanced forwarding policy.

As shown in Figure 7- 3, load balancing routes are configured respectively on R 1 and R 3 so that packets sent to the network segment of PC 3 or PC 1 are balanced between two routes, including a route through R 2 and a route through R 4.

- On R 1, configure two routes to the network segment of PC 3, including a route through R 2 and a route through R 4.
- On R 3, configure two routes to the network segment of PC 1, including a route through R 2 and a route through R 4.

Figure 7- 3



Remarks	On the switch, the load is balanced based on the source.

Deployment

- Configure the address and subnet mask of each interface.
- Configure static routes on R 1, R 2, R 3, and R 4.
- Configure the load balancing policy on R 1 and R 3.

7.3 Features

Feature	Description
Route Computation	Generate a valid route on a device.
Optimal Route Selection	Select an optimal route to forward packets.
Default Route	Forward all packets and help reduce the size of a routing table.
Route Reliability	Quickly detect a route failure and recover communication.

7.3.1 Route Computation

Routing Function

Routing functions are classified into IPv4 and IPv6 routing functions. If the routing functions are disabled, a device is equivalent to a host and cannot forward routes.

Dynamic Route

A dynamic routing protocol learns remote routes and dynamically updates routes by exchanging routes with neighbors. If a neighbor is the next hop of a route and this neighbor fails, the route fails as well.

Static Route

On a network with a simple topology, you can configure only static routes to implement network interworking. Appropriate configuration and use of static routes can improve the network performance and guarantee the bandwidth for important network applications.

Whether a static route is active is computed based on the status of the local interface. When the exit interface of a static route is located at layer 3 (L3) and is in Up status (the link status is Up and the IP address is configured), this route is active and can be used for packet forwarding.

7.3.2 Optimal Route Selection

Administrative Distance

When multiple routing protocols generate routes to the same destination, the priorities of these routes can be determined based on the administrative distance. A smaller administrative distance indicates a higher priority.

Equal-Cost Route

If multiple routes to the same destination have different next hops but the same administrative distance, these routes are mutually equal-cost routes. Packets are distributed among these routes to implement load balancing based on the balanced forwarding policy.

On a specific device, the total number of equal-cost routes is limited. Routes beyond the limit do not participate in packet forwarding.

Floating Route

If multiple routes to the same destination have different next hops and different administrative distances, these routes are mutually floating routes. The route with the smallest administrative distance will be first selected for packet forwarding. If this route fails, a route with a larger administrative distance is further selected for forwarding, thus preventing communication interruption caused by a network line failure.

7.3.3 Default Route

In the forwarding routing table, the route with the destination network segment 0.0.0.0 and the subnet mask 0.0.0.0 is the default route. Packets that cannot be forwarded by other routes will be forwarded by the default route. The default route can be statically configured or generated by a dynamic routing protocol.

Default Gateway

On a L2 switch, the **ip default gateway** command is configured to generate a default route.

Static Default Route

On a L3 switch, a static route with the network segment 0.0.0.0 and the subnet mask 0.0.0.0 is configured to generate the default route.

Default Network

The default network is configured to generate a default route. If the **ip default-network** command is configured to specify a network (a classful network, such as a Class A, B, or C network), and this network exists in the routing table, the router will use this network as the default network and the next hop of this network is the default gateway. As the network specified by the **ip default-network** command is a classful one, if this command is used to identify a subnet in a classful network, the router automatically generates a static route of the classful network instead of any default route.

7.3.4 Route Reliability

When a device on a network is faulty, some routes become unreachable, resulting in traffic interruption. If connectivity of the next hop can be detected in real time, the route can be re-computed when a fault occurs, or traffic can be switched over to the standby route.

Correlation with Track

A track object is an abstract concept. It can be used to trace whether an IP address is reachable or whether an interface is up. If a dynamic routing protocol or a static route is correlated with the Track function, the dynamic routing protocol or the static route can quickly learn whether the next hop is reachable so as to respond quickly.

7.4 Configuration

Configuration Item	Description and Command	
Configuring a Static Route	(Mandatory) It is used to configure a static route entry.	
	ip route	Configures an IPv4 static route.
	ipv6 route	Configures an IPv6 static route.
Configuring a Default Route	(Optional) It is used to configure the default gateway.	
	ip default gateway	Configures an IPv4 default gateway on a L2 device.

Configuration Item	Description and Command	
	ipv6 default gateway	Configures an IPv6 default gateway on a L2 device.
	ip route 0.0.0.0 0.0.0.0 *gateway*	Configures an IPv4 default gateway on a L3 device.
	ipv6 route ::/0 *ipv6-gateway*	Configures an IPv6 default gateway on a L3 device.
	ip default network	Configures an IPv4 default network on a L3 device.
Configuring Route Limitations	(Optional) It is used to limit the number of equal-cost routes and number of static routes, or disable routing.	
	maximum-paths	Configures the maximum number of equal-cost routes.
	ip static route-limit	Configures the maximum number of IPv4 static routes.
	ipv6 static route-limit	Configures the maximum number of IPv6 static routes.
	no ip routing	Disables IPv4 routing.
	no ipv6 unicast-routing	Disables IPv6 routing.

7.4.1 Configuring a Static Route

Configuration Effect

- Generate a static route in the routing table. Use the static route to forward packets to a remote network.

Notes

- Static routes cannot be configured on a L2 switch.
- If the **no ip routing** command is configured on a L3 switch, you cannot configure IPv4 static routes on this switch, and existing IPv4 static routes will also be deleted. Before the device is restarted, reconfiguring the **ip routing** command can recover the deleted IPv4 static routes. After the device is restarted, deleted IPv4 static routes cannot be recovered.
- If the **no ipv6 unicast- routing** command is configured on a L3 switch, you cannot configure IPv6 static routes on this switch, and existing IPv6 static routes will also be deleted. Before the device is restarted, reconfiguring the **ipv6 unicast- routing** command can recover the deleted IPv6 static routes. After the device is restarted, deleted IPv6 static routes cannot be recovered.

Configuration Steps

Configuring a Static IPv4 Route

Configure the following command on an IPv4-enabled router.

Command	**ip route***network net-mask* {*ip-address* | *interface* [*ip-address*]} [*distance*] [**tag** *tag*] [**permanent** | **track** *object-number*] [**weight** *number*] [**description***description-text*] [**disabled** | **enabled**]	
Parameter Description	*network*	Indicates the address of the destination network.
	net-mask	Indicates the mask of the destination network.

	ip-address	(Optional) Indicates the next-hop address of the static route. You must specify at least one of *ip-address* and *interface,* or both of them. If *ip-address* is not specified, a static direct route is configured.
	interface	(Optional) Indicates the next-hop exit interface of the static route. You must specify at least one of *ip-address* and *interface,* or both of them. If *interface* is not specified, a recursive static direct route is configured. The exit interface is obtained by the next hop in the routing table.
	distance	(Optional) Indicates the administrative distance of the static route. The administrative distance is 1 by default.
	tag	(Optional) Indicates the tag of the static route. The tag is 0 by default.
	permanent	(Optional) Indicates the flag of the permanent route. The static route is not a permanent route by default.
	track *object-number*	(Optional) Indicates correlation with Track. *object-number* indicates the ID of the track object. By default, the static route is not correlated with the Track function.
	weight *number*	(Optional) Indicates the weight of the static route. The weight is 1 by default.
	description*description-text*	(Optional) Indicates the description of the static route. By default, no description is configured. *description-text* is a string of one to 60 characters.
	disabled/enabled	(Optional) Indicates the enable flag of the static route. The flag is enabled by default.
Defaults	By default, no static route is configured.	
Command Mode	Global configuration mode	
Usage Guide	The simplest configuration of this command is **ip route** *networknet-maskip-address.* If the static route is correlated with Track and the down status of the trace object is detected, the static route is not active and does not participate in packet forwarding.	

Configuring an IPv6 Static Route

Configure the following command on an IPv6-enabled router.

Command	**ipv6 route** [**vrf***vrf-name*] *ipv6-prefix*/*prefix-length* { *ipv6-address* [**nexthop-vrf** {*vrf-name1*/**default**}] | *interface* [*ipv6-address* [**nexthop-vrf** {*vrf-name1*/**default**}]] } [*distance*] [**weight***number*] [**description***description-text*]	
Parameter Description	**vrf***vrf-name*	(Optional) Indicates the routing VRF, which must be a multi-protocol VRF of a configured IPv6 address family. The VRF is a global VRF by default.
	ipv6-prefix	Indicates the IPv6 prefix, which must comply with the address expression specified in RFC4291.
	prefix-length	Indicates the length of the IPv6 prefix. Note that a slash (/) must be added in front of the length.
	ipv6-address	(Optional) Indicates the next-hop address of the static route. You must specify at least one of *ipv6-address* and *interface,* or both of them. If *ipv6-address* is not specified, a static direct route is configured.
	interface	(Optional) Indicates the next-hop exit interface of the static route. You must specify at least one of *ipv6-address* and *interface,* or both of them. If *interface* is not specified, a recursive static direct route is configured. The exit interface is obtained by the next hop in the routing table.
	nexthop-vrf *vrf-name1*	(Optional) Indicates the routing VRF of the next hop, which must be a multi-protocol VRF of a configured IPv6 address family. By default, the VRF of the next hop is the same as the VRF specified by the VRF name. **nexthop-vrf default** indicates that the VRF of the next shop is a global VRF.

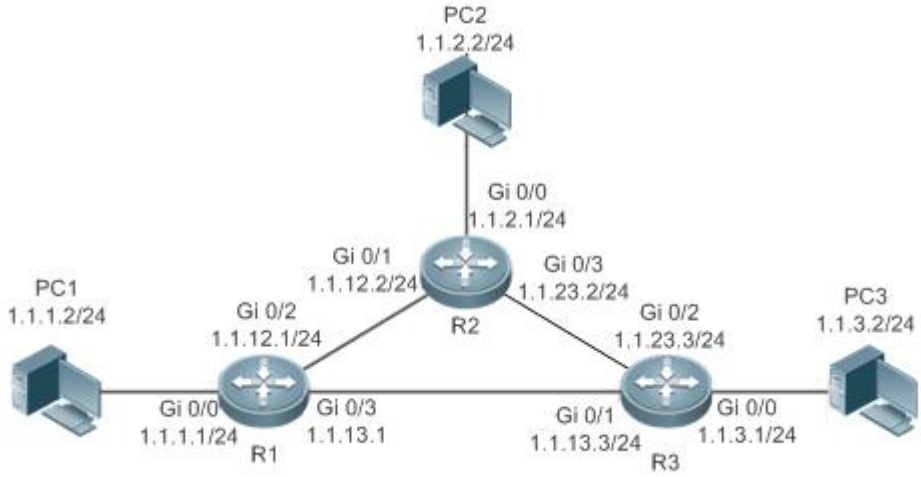
	distance	(Optional) Indicates the administrative distance of the static route. The administrative distance is 1 by default.
	weight *number*	(Optional) Indicates the weight of the static route, which must be specified when you configure equal-cost routes. The weight ranges from 1 to 8. When the weights of all equal-cost routes of a route are summed up, the sum cannot exceed the maximum number of equal-cost routes that can be configured for the route. Weighting of equal-cost routes of a route indicates the traffic ratio of these routes. The weight is 1 by default.
	description*descripti on-text*	(Optional) Indicates the description of the static route. By default, no description is configured. *description-text* is a string of one to 60 characters.
Defaults	By default, no static route is configured.	
Command Mode	Global configuration mode	
Usage Guide	The simplest configuration of this command is **ipv6 route***ipv6-prefix* / *prefix-lengthipv6-address.*	

Verification

- Run the **show ip route** command to display the IPv4 routing table and check whether the configured IPv4 static route takes effect.
- Run the **show ipv6 route** command to display the IPv6 routing table and check whether the configured IPv6 static route takes effect.

Configuration Example

Configuring Static Routes to Implement Interworking of the IPv4 Network

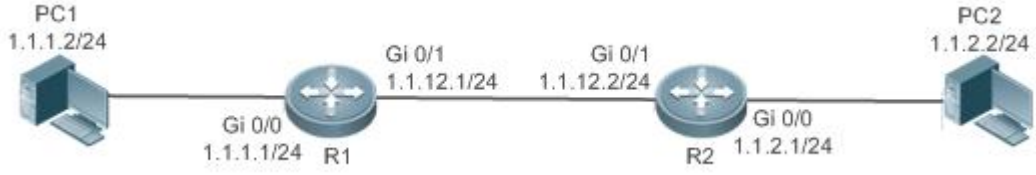
Scenario **Figure 7-4**	
Configuration Steps	● Configure interface addresses on each device.
R1	R1#configure terminal R1(config)#interface gigabitEthernet 0/0 R1(config-if-GigabitEthernet 0/0)# ip address 1.1.1.1 255.255.255.0 R1(config-if-GigabitEthernet 0/0)# exit

	R1(config)#interface gigabitEthernet 0/2 R1(config-if-GigabitEthernet 0/2)# ip address 1.1.12.1 255.255.255.0 R1(config-if-GigabitEthernet 0/0)# exit R1(config)#interface gigabitEthernet 0/3 R1(config-if-GigabitEthernet 0/3)# ip address 1.1.13.1 255.255.255.0
R2	R2#configure terminal R2(config)#interface gigabitEthernet 0/0 R2(config-if-GigabitEthernet 0/0)# ip address 1.1.2.1 255.255.255.0 R2(config-if-GigabitEthernet 0/0)# exit R2(config)#interface gigabitEthernet 0/1 R2(config-if-GigabitEthernet 0/1)# ip address 1.1.12.2 255.255.255.0 R2(config-if-GigabitEthernet 0/0)# exit R2(config)#interface gigabitEthernet 0/3 R2(config-if-GigabitEthernet 0/3)# ip address 1.1.23.2 255.255.255.0
R3	R3#configure terminal R3(config)#interface gigabitEthernet 0/0 R3(config-if-GigabitEthernet 0/0)# ip address 1.1.3.1 255.255.255.0 R3(config-if-GigabitEthernet 0/0)# exit R3(config)#interface gigabitEthernet 0/1 R3(config-if-GigabitEthernet 0/1)# ip address 1.1.13.3 255.255.255.0 R3(config-if-GigabitEthernet 0/0)# exit R3(config)#interface gigabitEthernet 0/2 R3(config-if-GigabitEthernet 0/2)# ip address 1.1.23.3 255.255.255.0
	● Configure static routes on each device.
R1	R1#configure terminal R1(config)#ip route 1.1.2.0 255.255.255.0 GigabitEthernet 0/2 1.1.12.2 R1(config)# ip route 1.1.3.0 255.255.255.0 GigabitEthernet 0/3 1.1.13.3
R2	R2#configure terminal R2(config)#ip route 1.1.1.0 255.255.255.0 GigabitEthernet 0/1 1.1.12.1 R2(config)# ip route 1.1.3.0 255.255.255.0 GigabitEthernet 0/3 1.1.23.3
R3	R3#configure terminal R3(config)#ip route 1.1.2.0 255.255.255.0 GigabitEthernet 0/2 1.1.23.2

	R3(config)# ip route 1.1.1.0 255.255.255.0 GigabitEthernet 0/1 1.1.13.1
Verification	● Display the routing table.
R1	R1# show ip route Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, * - candidate default Gateway of last resort is no set C 1.1.1.0/24 is directly connected, GigabitEthernet 0/0 C 1.1.1.1/32 is local host. S 1.1.2.0/24 [1/0] via 1.1.12.2, GigabitEthernet 0/2 S 1.1.3.0/24 [1/0] via 1.1.13.3, GigabitEthernet 0/2 C 1.1.12.0/24 is directly connected, GigabitEthernet 0/2 C 1.1.12.1/32 is local host. C 1.1.13.0/24 is directly connected, GigabitEthernet 0/3 C 1.1.13.1/32 is local host.
R2	R2# show ip route Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, * - candidate default Gateway of last resort is no set S 1.1.1.0/24 [1/0] via 1.1.12.1, GigabitEthernet 0/0 C 1.1.2.0/24 is directly connected, GigabitEthernet 0/0 C 1.1.2.1/32 is local host. S 1.1.3.0/24 [1/0] via 1.1.23.3, GigabitEthernet 0/3

	C 1.1.12.0/24 is directly connected, GigabitEthernet 0/1 C 1.1.12.2/32 is local host. C 1.1.23.0/24 is directly connected, GigabitEthernet 0/3 C 1.1.23.2/32 is local host.
R3	R3# show ip route Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, * - candidate default Gateway of last resort is no set S 1.1.1.0/24 [1/0] via 1.1.13.1, GigabitEthernet 0/2 S 1.1.2.0/24 [1/0] via 1.1.23.2, GigabitEthernet 0/2 C 1.1.3.0/24 is directly connected, GigabitEthernet 0/0 C 1.1.3.1/32 is local host. C 1.1.13.0/24 is directly connected, GigabitEthernet 0/1 C 1.1.13.3/32 is local host. C 1.1.23.0/24 is directly connected, GigabitEthernet 0/2 C 1.1.23.3/32 is local host.

Correlating IPv4 Static Routes with Track

Scenario Figure 7- 5	
Configuration Steps	● Configure static routes on R 1 and R 2, and specify the exit interface or next hop as the interworking interface. ● Correlate static routes with Track on R 1 and R 2, and check the connectivity of the next hops of static routes. ●
R1	R1#configure terminal R1(config)#interface gigabitEthernet 0/1 R1(config-if-GigabitEthernet 0/1)# ip address 1.1.12.1 255.255.255.0 R1(config-if-GigabitEthernet 0/1)# exit

	R1(config)#track 2 interface gigabitEthernet 0/1 line-protocol R1(config)# ip route 1.1.2.0 255.0.0.0 gigabitEthernet 0/1 1.1.12.2 track 2
R2	R2#configure terminal R1(config)#interface gigabitEthernet 0/1 R1(config-if-GigabitEthernet 0/1)# ip address 1.1.12.2 255.255.255.0 R1(config-if-GigabitEthernet 0/1)# exit R1(config)#track 2 interface gigabitEthernet 0/1 line-protocol R1(config)# ip route 1.1.1.0 255.0.0.0 gigabitEthernet 0/1 1.1.12.1 track 2
Verification	● Display the Track status. ● Display the static routes correlated with Track. R1# show track 2 Track 2 Interface gigabitEthernet 0/1 The state is Up, delayed Down (5 secs remaining) 1 change, current state last: 300 secs Delay up 0 secs, down 0 secs R1#show ip route track-table ip route 1.1.2.0 255.0.0.0 GigabitEthernet 0/1 1.1.12.2 track 2 up

Configuring Static Routes to Implement Interworking of the IPv6 Network

Scenario Figure 7-6	
Configuration Steps	● Configure interface addresses on each device.
R1	R1#configure terminal R1(config)#interface gigabitEthernet 0/0 R1(config-if-GigabitEthernet 0/0)# ipv6 address 1111:1111::1/64 R1(config-if-GigabitEthernet 0/0)# exit R1(config)#interface gigabitEthernet 0/1

	R1(config-if-GigabitEthernet 0/1)# ipv6 address 1111:1212::1/64
R2	R2#configure terminal R2(config)#interface gigabitEthernet 0/0 R2(config-if-GigabitEthernet 0/0)#ipv6 address 1111:2323::1/64 R2(config-if-GigabitEthernet 0/0)# exit R2(config)#interface gigabitEthernet 0/1 R2(config-if-GigabitEthernet 0/1)# ipv6 address 1111:1212::2/64
	● Configure static routes on each device.
R1	R1#configure terminal R1(config)# ipv6 route 1111:2323::0/64 gigabitEthernet 0/1
R2	R2#configure terminal R2(config)#ipv6 route 1111:1111::0/64 gigabitEthernet 0/1
Verification	● Display the routing table.
R1	R1# show ipv6 route IPv6 routing table name - Default - 10 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area C 1111:1111::/64 via GigabitEthernet 0/0, directly connected L 1111:1111::1/128 via GigabitEthernet 0/0, local host C 1111:1212::/64 via GigabitEthernet 0/1, directly connected L 1111:1212::1/128 via GigabitEthernet 0/1, local host S 1111:2323::/64 [1/0] via GigabitEthernet 0/1, directly connected C FE80::/10 via ::1, Null0 C FE80::/64 via GigabitEthernet 0/0, directly connected L FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/0, local host C FE80::/64 via GigabitEthernet 0/1, directly connected

	L FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/1, local host
R2	R2# show ipv6 route IPv6 routing table name - Default - 10 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area C 1111:2323::/64 via GigabitEthernet 0/0, directly connected L 1111:2323::1/128 via GigabitEthernet 0/0, local host C 1111:1212::/64 via GigabitEthernet 0/1, directly connected L 1111:1212::1/128 via GigabitEthernet 0/1, local host S 1111:1111::/64 [1/0] via GigabitEthernet 0/1, directly connected C FE80::/10 via ::1, Null0 C FE80::/64 via GigabitEthernet 0/0, directly connected L FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/0, local host C FE80::/64 via GigabitEthernet 0/1, directly connected L FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/1, local host

Common Errors

- The link on the interface is not up.
- No IP address is configured for the interface.
- The static route is correlated with Track, but the track object is not configured.

7.4.2 Configuring a Default Route

Configuration Effect

- Generate a default route in the routing table. The default route is used to forward packets that cannot be forwarded by other routes.

Notes

- On a L2 switch, run the **ip default gateway** or **ipv6 default gateway** command to configure the default gateway.

- On a L3 switch, run the **ip route** 0.0.0.0 0.0.0.0 *gateway* or **ipv6 route** ::/0 *ipv6-gateway*command to configure the default gateway.
- If the **no ip routing** or **no ipv6 unicast- routing** command is configured on a L3 switch, you can run the **ip default gateway** or **ipv6 default gateway** command to configure the default gateway.

Configuration Steps

Configuring the IPv4 Gateway on a L2 Switch

Command	**ip default-gateway***gateway*	
Parameter Description	*gateway*	indicates the IPv4 gateway address.
Defaults	By default, no static default route is configured.	
Command Mode	Global configuration mode	
Usage Guide	N/A	

Configuring the IPv6 Gateway on a L2 Switch

Command	**ipv6 default-gateway***gateway*	
Parameter Description	*gateway*	indicates the IPv6 gateway address.
Defaults	By default, no static default route is configured.	
Command Mode	Global configuration mode	
Usage Guide	N/A	

Configuring the IPv4 Default Gateway on a L3 Switch

Command	**ip route0.0.0.00.0.0.0**{*ip-address* | *interface* [*ip-address*]} [*distance*] [**tag** *tag*] [**permanent**] [**weight** *number*] [**description***description-text*] [**disabled** | **enabled**]	
Parameter Description	**0.0.0.0**	Indicates the address of the destination network.
	0.0.0.0	Indicates the mask of the destination network.
	ip-address	(Optional) Indicates the next-hop address of the static route. You must specify at least one of *ip-address* and *interface,* or both of them. If *ip-address* is not specified, a static direct route is configured.
	interface	(Optional) Indicates the next-hop exit interface of the static route. You must specify at least one of *ip-address* and *interface,* or both of them. If *interface* is not specified, a recursive static direct route is configured. The exit interface is obtained by the next hop in the routing table.
	distance	(Optional) Indicates the administrative distance of the static route. The administrative distance is 1 by default.
	tag	(Optional) Indicates the tag of the static route. The tag is 0 by default.
	permanent	(Optional) Indicates the flag of the permanent route. The static route is not a permanent route by default.
	weight *number*	(Optional) Indicates the weight of the static route. The weight is 1 by default.
	description*description -text*	(Optional) Indicates the description of the static route. By default, no description is configured. *description-text* is a string of one to 60 characters.

	disabled /enabled	(Optional) Indicates the enable flag of the static route. The flag is enabled by default.
Defaults	By default, no static default route is configured.	
Command Mode	Global configuration mode	
Usage Guide	The simplest configuration of this command is **ip route0.0.0.0 0.0.0.0** *ip-address.*	

Configuring the IPv6 Default Gateway on a L3 Switch

Command	**ipv6 route** [**vrf***vrf-name*] **::/0** { *ipv6-address* [**nexthop-vrf** {*vrf-name1*/**default**}] | *interface* [*ipv6-address* [**nexthop-vrf** {*vrf-name1*/**default**}]] } [*distance*] [**weight***number*] [**description***description-text*]	
Parameter Description	**vrf***vrf-name*	(Optional) Indicates the routing VRF, which must be a multi-protocol VRF of a configured IPv6 address family. The VRF is a global VRF by default.
	::	Indicates the IPv6 prefix, which must comply with the address expression specified in RFC4291.
	0	Indicates the length of the IPv6 prefix. Note that a slash (/) must be added in front of the length.
	Ipv6-address	(Optional) Indicates the next-hop address of the static route. You must specify at least one of *ipv6-address* and *interface,* or both of them. If *ipv6-address* is not specified, a static direct route is configured.
	interface	(Optional) Indicates the next-hop exit interface of the static route. You must specify at least one of *ipv6-address* and *interface,* or both of them. If *interface* is not specified, a recursive static direct route is configured. The exit interface is obtained by the next hop in the routing table.
	nexthop-vrf *vrf-name1*	(Optional) Indicates the routing VRF of the next hop, which must be a multi-protocol VRF of a configured IPv6 address family. By default, the VRF of the next hop is the same as the VRF specified by *vrf name*. **nexthop-vrf default** indicates that the VRF of the next shop is a global VRF.
	distance	(Optional) Indicates the administrative distance of the static route. The administrative distance is 1 by default.
	weight *number*	(Optional) Indicates the weight of the static route, which must be specified when you configure equal-cost routes. The weight ranges from 1 to 8. When the weights of all equal-cost routes of a route are summed up, the sum cannot exceed the maximum number of equal-cost routes that can be configured for the route. Weighting of equal-cost routes of a route indicates the traffic ratio of these routes. The weight is 1 by default.
	description*descriptio n-text*	(Optional) Indicates the description of the static route. By default, no description is configured. *description-text* is a string of one to 60 characters.
Defaults	By default, no static default route is configured.	
Command Mode	Global configuration mode	
Usage Guide	The simplest configuration of this command is **ipv6 route** ::/0 *ipv6-gateway.*	

Configuring the IPv4 Default Network on a L3 Switch

Command	**ip default-network** *network*	
Parameter Description	*network*	Indicates the address of the network. (The network must be a Class A, B, or C network.)
Defaults	By default, no default network is configured.	
Command	Global configuration mode	

Mode	
Usage Guide	If the network specified by the **ip default-network** command exists, a default route is generated and the next hop to this network is the default gateway. If the network specified by the **ip default-network** command does not exist, the default route is not generated.

Verification

- On a L2 switch (or a L3 switch where routing is disabled), run the **show ip redirects** or **show ipv6 redirects** command to display the default gateway.
- On a L3 switch where routing is enabled, run the **show ip route** or **show ipv6 route** command to display the default route.

Configuration Example

Configuring IPv4 Default Routes on L3 Switches to Implement Network Interworking

Scenario Figure 7-7	
Configuration Steps	● Configure IP addresses on L3 devices.
R1	R1#configure terminal R1(config)#interface gigabitEthernet 0/0 R1(config-if-GigabitEthernet 0/0)# ip address 1.1.1.1 255.255.255.0 R1(config-if-GigabitEthernet 0/0)# exit R1(config)#interface gigabitEthernet 0/1 R1(config-if-GigabitEthernet 0/1)# ip address 1.1.12.1 255.255.255.0 R1(config-if-GigabitEthernet 0/0)# exit
R2	R2#configure terminal R2(config)#interface gigabitEthernet 0/0 R2(config-if-GigabitEthernet 0/0)# ip address 1.1.2.1 255.255.255.0 R2(config-if-GigabitEthernet 0/0)# exit R2(config)#interface gigabitEthernet 0/1 R2(config-if-GigabitEthernet 0/1)# ip address 1.1.12.2 255.255.255.0 R2(config-if-GigabitEthernet 0/0)# exit
R1	● Configure an IPv6 default gateway on R 1. R1#configure terminal

	R1(config)#ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/1 1.1.12.2
R2	R2#configure terminal R2(config)#ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/1 1.1.12.1
Verification	● Display the routing table.
R1	R1# show ip route Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, * - candidate default Gateway of last resort is 1.1.12.2 S* 0.0.0.0/0 [1/0] via 1.1.12.2, GigabitEthernet 0/1 C 1.1.1.0/24 is directly connected, GigabitEthernet 0/0 C 1.1.1.1/32 is local host. C 1.1.12.0/24 is directly connected, GigabitEthernet 0/1 C 1.1.12.1/32 is local host.

7.4.3 Configuring Route Limitations

Configuration Effect

- Limit the number of equal-cost routes and number of static routes, or disable routing.

Notes

Route limitations cannot be configured on a L2 switch.

Configuration Steps

↘ **Configuring the Maximum Number of Equal-Cost Routes**

Command	**maximum-paths***number*	
Parameter Description	*number*	Indicates the maximum number of equal-cost routes. The value ranges from 1 to 64 (vary with products).
Defaults	The default value varies with products.	
Command Mode	Global configuration mode	

Usage Guide	Run this command to configure the maximum number of next hops in the equal-cost route. In load balancing mode, the number of routes on which traffic is balanced does not exceed the configured number of equal-cost routes.

Configuring the Maximum Number of IPv4 Static Routes

Command	**ip static route-limit***number*	
Parameter Description	*number*	Indicates the upper limit of routes. The value ranges from 1 to 10,000.
Defaults	By default, a maximum of 1,024 IP static routes can be configured.	
Command Mode	Global configuration mode	
Usage Guide	Run this command to configure the maximum number of IPv4 static routes. If the maximum number of IPv4 static routes is reached, no more IPv4 static route can be configured.	

Configuring the Maximum Number of IPv6 Static Routes

Command	**ipv6 static route-limit** *number*	
Parameter Description	*number*	Indicates the upper limit of routes. The value ranges from 1 to 10,000.
Defaults	By default, a maximum of 1,000 IPv6 static routes can be configured.	
Command Mode	Global configuration mode	
Usage Guide	Run this command to configure the maximum number of IPv6 static routes. If the maximum number of IPv6 static routes is reached, no more IPv6 static route can be configured.	

Disabling IPv4 Routing

Command	**no ip routing**
Parameter Description	N/A
Defaults	By default, IPv4 routing is enabled.
Command Mode	Global configuration mode
Usage Guide	Run this command to disable IPv4 routing. If the device functions only as a bridge or a voice over IP (VoIP) gateway, the device does not need to use the IPv4 routing function of the FSOS software. In this case, you can disable the IPv4 routing function of the FSOS software.

Disabling IPv6 Routing

Command	**no ipv6 unicast-routing**
Parameter Description	N/A
Defaults	By default, IPv6 routing is enabled.
Command Mode	Global configuration mode
Usage Guide	Run this command to disable IPv6 routing. If the device functions only as a bridge or a VoIP gateway, the device does not need to use the IPv6 routing function of the FSOS software. In this case, you can disable the IPv6 routing function of the

	FSOS software.

7.5 Monitoring

Displaying

Description	Command
Displays the IPv4 routing table.	**show ip route**
Displays the IPv6 routing table.	**show ipv6 route**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs IPv4 route management.	**debug nsm kernel ucast- v4**
Debugs default network management.	**debug nsm kernel default-network**
Debugs internal events of route management.	**debug nsm events**
Debugs sending of route management and routing protocol messages.	**debug nsm packet send**
Debugs receiving of route management and routing protocol messages.	**debug nsm packet recv**

Chapter 11 Security Configuration

1. Configuring the ACL
2. Configuring RPL
3. Configuring RNFP
4. Configuring SSH
5. Configuring DHCP Snooping
6. Configuring ARP Check
7. Configuring IP Source Guard
8. Configuring SEC-VPDN
9. Configuring IPSec
10. Configuring IKE
11. Configuring ITBOX
12. Configuring AAA
13. Configuring RADIUS
14. Configuring TACACS+
15. Configuring Web Authentication
16. Configuring Global IP-MAC Binding
17. Configuring IPoE
18. Configuring IP Group
19. Configuring Link-SAM
20. Configuring Flow Account
21. Configuring APP-AUTH
22. Configuring Webservice
23. Configuring ANTI-PAP
24. Configuring WEB-ADVERT
25. Configuring Local-account
26. Configuring Firewall

1 Configuring the ACL

1.1 Overview

Access control list (ACL) is also called access list or firewall. It is even called packet filtering in some documents. The ACL defines rules to determine whether to forward or drop data packets arriving at a network interface.

ACLs are classified by function into two types:

- Security ACLs: Used to control data flows that are allowed to pass through a network device.
- Quality of service (QoS) ACLs: Used to classify and process data flows by priority.

ACLs are configured for a lot of reasons. Major reasons include:

- Network access control: To ensure network security, rules are defined to limit access of users to some services (for example, only access to the WWW and email services is permitted, and access to other services such as Telnet is prohibited), or to allow users to access services in a specified period of time, or to allow only specified hosts to access the network.
- QoS: QoS ACLs are used to preferentially classify and process important data flows. For details about the use of QoS ALCs, see the configuration manual related to QoS.

1.2 Applications

Application	Description
Access Control of an Enterprise Network	On an enterprise network, the network access rights of each department, for example, access rights of servers and use permissions of chatting tools (such as QQ and MSN), must be controlled according to requirements.

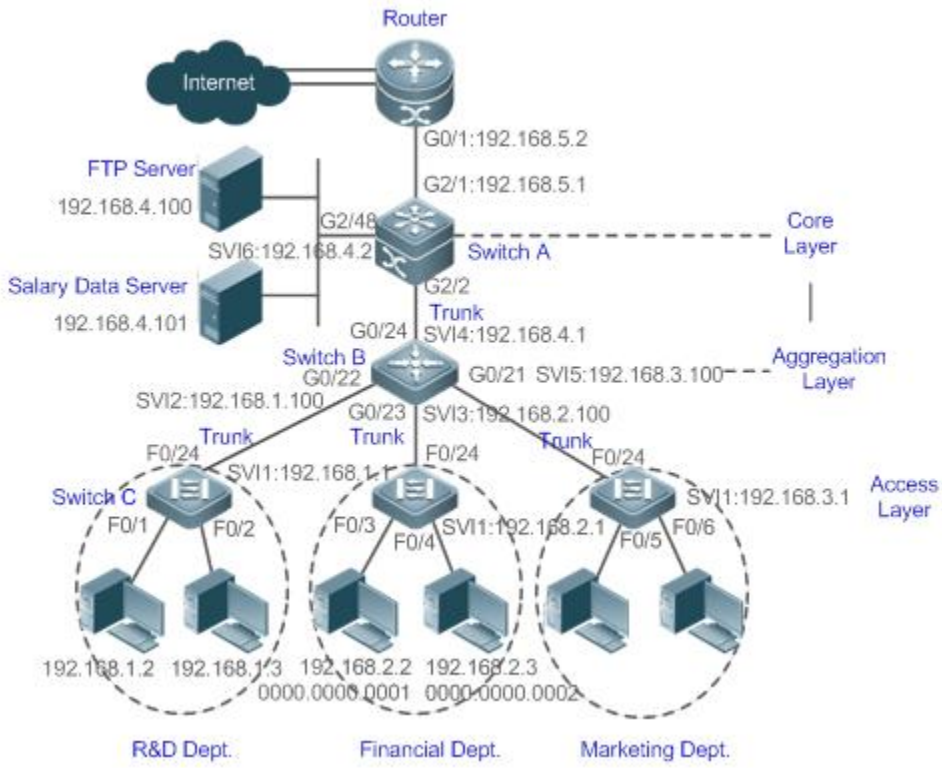
1.2.1 Access Control of an Enterprise Network

Scenario

Internet viruses can be found everywhere. Therefore, it is necessary to block ports that are often used by viruses to ensure security of an enterprise network as follows:

- Allow only internal PCs to access the server.
- Prohibit PCs of a non-financial department from accessing PCs of the financial department, and prohibit PCs of a non-R&D department from accessing PCs of the R&D department.
- Prohibit the staff of the R&D department from using chatting tools (such as QQ and MSN) during working hours from 09:00 to 18:00.

Figure 1-1



Remarks	Switch C at the access layer: It is connected to PCs of each department and to Switch B at the aggregation layer through the gigabit optical fiber (trunk mode). Switch B at the aggregation layer: Multiple virtual local area networks (VLANs) are divided. One VLAN is defined for one department. These VLANs are connected to Switch A at the core layer through the 10-gigabit optical fiber (trunk mode). Switch A at the core layer: It is connected to various servers, such as the File Transfer Protocol (FTP) server and Hypertext Transfer Protocol (HTTP) server, and to the Internet through firewalls.

Deployment

- Configure an extended ACL on the port G2/1 to filter data packets, thus protecting the network against the viruses. This port is located on a core-layer device (Switch A) and used to connect Switch A to the uplink port G2/1 of a router.
- Allow only internal PCs to access servers, and prohibit external PCs from accessing servers. Define and apply the extended IP ACLs on G2/2 or switch virtual interface (SVI) 2 that is used to connect Switch A to an aggregation layer device or server.
- Prohibit mutual access between specified departments. Define and apply the extended IP ACLs on G0/22 and G0/23 of Switch B.
- Configure and apply the time-based extended IP ACLs on SVI 2 of Switch B to prohibit the R&D department from using chatting tools (such as QQ and MSN) in a specified period of time.

1.3 Features

Basic Concepts

ACL

ACLs include basic ACLs and dynamic ACLs.

You can select basic or dynamic ACLs as required. Generally, basic ACLs can meet the security requirements. However, experienced hackers may use certain software to access the network by means of IP address spoofing. If dynamic ACLs are used, users are requested to pass identify authentication before accessing the network, which prevents hackers from intruding the network. Therefore, you can use dynamic ACLs in some sensitive areas to guarantee network security.

IP address spoofing is an inherent problem of all ACLs, including dynamic ACLs. Hackers may use forged IP addresses to access the network during the validity period of authenticated user identities. Two methods are available to resolve this problem. One is to set the idle time of user access to a smaller value, which increases the difficulty in intruding networks. The other is to encrypt network data using the IPSec protocol, which ensures that all data is encrypted when arriving at a device.

ACLs are generally configured on the following network devices:

- Devices between the internal network and the external network (such as the Internet)
- Devices on the border of two network segments
- Devices connected to controlled ports

ACL statements must be executed in strict compliance with their sequence in the ACL. Comparison starts from the first statement. Once the header of a data packet matches a statement in the ACL, the subsequent statements are ignored and no longer checked.

Input/Output ACLs, Filtering Field Template, and Rules

When receiving a packet on an interface, the device checks whether the packet matches any access control entry (ACE) in the input ACL of this interface. Before sending a packet through a interface, the device checks whether the packet matches any ACE in the output ACL of this interface.

When different filtering rules are defined, all or only some rules may be applied simultaneously. If a packet matches an ACE, this packet is processed according to the action policy (permit or deny) defined in this ACE. ACEs in an ACL identify Ethernet packets based on the following fields in the Ethernet packets:

Layer 2 (L2) fields:

- 48-bit source MAC address (containing all 48 bits)
- 48-bit destination MAC address (containing all 48 bits)
- 16-bit L2 type field

Layer 3 (L3) fields:

- Source IP address field (All source IP address values can be specified, or the subnet can be used to define a type of data flows.)

- Destination IP address field (All destination IP address values can be specified, or the subnet can be used to define a type of data flows.)
- Protocol type field

Layer 4 (L4) fields:

- Either a TCP source or destination port is specified, or both are specified, or the range of the source or destination port is specified.
- Either a UDP source or destination port is specified, or both are specified, or the range of the source or destination port is specified.

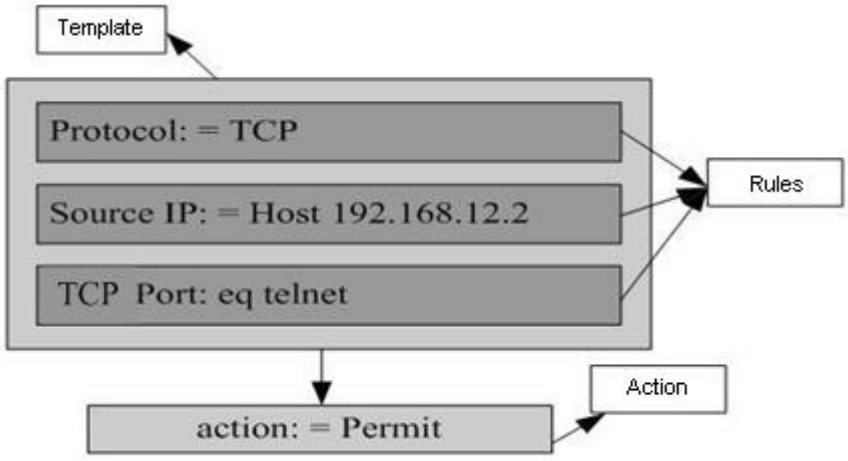
Filtering fields refer to the fields in packets that can be used to identify or classify packets when an ACE is generated. A filtering field template is a combination of these fields. For example, when an ACE is generated, packets are identified and classified based on the destination IP address field in each packet; when another ACE is generated, packets are identified and classified based on the source IP address field and UDP source port field in each packet. The two ACEs use different filtering field templates.

Rules refer to values of fields in the filtering field template of an ACE. For example, the content of an ACE is as follows:

```
permit tcp host 192.168.12.2 any eq telnet
```

In this ACE, the filtering field template is a combination of the following fields: source IP address field, IP protocol field, and TCP destination port field. The corresponding values (rules) are as follows: source IP address = Host 192.168.12.2; IP protocol = TCP; TCP destination port = Telnet.

Figure 1-2 Analysis of the ACE: permit tcp host 192.168.12.2 any eq telnet



A filtering field template can be a combination of L3 and L4 fields, or a combination of multiple L2 fields. The filtering field template of a standard or an extended ACL, however, cannot be a combination of L2 and L3 fields, a combination of L2 and L4 fields, or a combination of L2, L3, and L4 fields. To use a combination of L2,L3, and L4 fields, you can use the expert ACLs.

An SVI associated with ACLs in the outgoing direction supports the IP standard, IP extended, MAC extended, and expert ACLs.

If an MAC extended or expert ACL is configured to match the destination MAC address and is applied to the outgoing direction of the SVI, the related ACE can be configured but cannot take effect. If an IP extended or expert ACL is configured to match the destination IP address, but the destination IP address is not in the subnet IP address range of the associated SVI, the configured ACL cannot take effect. For example, assume that the address of VLAN 1 is **192.168.64.1 255.255.255.0**, an IP extended ACL is created, and the ACE is **deny udp any 192.168.65.1 0.0.0.255 eq 255**. If this ACL is applied to the outgoing interface of VLAN 1, the ACL cannot take effect because the destination IP address is not in the subnet IP address range of VLAN 1. If the ACE is **deny udp any 192.168.64.1 0.0.0.255 eq 255**, the ACL can take effect because the destination IP address is in the subnet IP address range of VLAN 1.

If ACEs of an ACL (IP ACL or expert extended ACL) are configured to match non-L2 fields (such as SIP and DIP), the ACL does not take effect on tagged MPLS packets.

ACL Logging

To allow users better learn the running status of ACLs on a device, you can determine whether to specify the ACL logging option as required when adding ACEs. If this option is specified, logs are output when packets matching ACEs are found. ACL logs are displayed based on ACEs. That is, the device periodically displays ACEs with matched packets and the number of matched packets. An example of the log is as follows:

```
*Sep   9 16:23:06: %ACL-6-MATCH: ACL 100 ACE 10 permit icmp any any, match 78 packets.
```

To control the amount of logs and output frequency, you can configure the log update interval respectively for the IPv4/IPv6 ACL.

An ACE containing the ACL logging option consumes more hardware resources. If all configured ACEs contain this option, the ACE capacity of a device will be reduced by half.

By default, the log update interval is 0, that is, no log is output. After the ACL logging option is specified in an ACE, you need to configure the log update interval to output related logs.

For an ACE containing the ACL logging option, if no packet is matched in the specified interval, no packet matching log related to this ACE will be output. If matched packets are found in the specified interval, packet matching logs related to this ACE will be output when the interval expires. The number of matched packets is the total number of packets that match the ACE during the specified interval, that is, the period from the previous log output to the current log output.

Only switches support the ACL logging function.

ACL Packet Matching Counters

To implement network management, users may want to know whether an ACE has any matched packets and how many packets are matched. ACLs provide the ACE-based packet matching counters. You can enable or disable packet matching counters for all ACEs in an ACL, which can be an IP ACL, MAC ACL, expert ACL or IPv6 ACL. In addition, you can run the **clear counters access-list** [*acl-id* | *acl-name*] command to reset ACL counters for a new round of statistics.

Enabling ACL counters requires more hardware entries. In an extreme case, this will reduce by half the number of ACEs that can be configured on a device.

Only switches support the ACL packet matching counters.

Overview

Feature	Description
IP ACL	Control incoming or outgoing IPv4 packets of a device based on the L3 or L4 information in the IPv4 packet header.
IPv6 ACL	Control incoming or outgoing IPv6 packets of a device based on the L3 or L4 information in the IPv6 packet header.
ACL Logging	Output ACL packet matching logs at a specified interval according to requirements. The logs help users learn the packet matching result of a specified ACE.

1.3.1 IP ACL

The IP ACL implements refined control on incoming and outgoing IPv4 packets of a device. You can permit or deny the entry of specific IPv4 packets to a network according to actual requirements to control access of IP users to network resources.

Working Principle

Define a series of IP access rules in the IP ACL, and then apply the IP ACL either in the incoming or outgoing direction of an interface or globally. The device checks whether the incoming or outgoing IPv4 packets match the rules and accordingly forwards or blocks these packets.

To configure an IP ACL, you must specify a unique name or ID for the ACL of a protocol so that the protocol can uniquely identify each ACL. The following table lists the protocols that can use IDs to identify ACLs and the range of IDs.

Protocol	ID Range
Standard IP	1–99, 1300–1999
Extended IP	100–199, 2000–2699

Basic ACLs include the standard IP ACLs and extended IP ACLs. Typical rules defined in an ACL contain the following matching fields:

- Source IP address
- Destination IP address
- IP protocol number
- L4 source port ID or ICMP type
- L4 destination port ID or ICMP code

The standard IP ACL (ID range: 1–99, 1300–1999) is used to forward or block packets based on the source IP address, whereas the extended IP ACL (ID range: 100–199, 2000–2699) is used to forward or block packets based on a combination of the preceding matching fields.

For an individual ACL, multiple independent ACL statements can be used to define multiple rules. All statements reference the same ID or name so that these statements are bound with the same ACL. However, more statements mean that it is increasingly difficult to read and understand the ACL.

For routing products, the ICMP code matching field in an ACE is ineffective for ICPM packets whose ICPM type is 3. If the ICPM code of ICMP packets to be matched is configured in an ACE, the ACL matching result of incoming ICMP packets of a device whose ICPM type is 3 may be different from the expected result.

Implicit "Deny All Traffic" Rule Statement

At the end of every IP ACL is an implicit "deny all traffic" rule statement. Therefore, if a packet does not match any rule, the packet will be denied.

For example:

```
access-list 1 permit host 192.168.4.12
```

This ACL permits only packets sent from the source host 192.168.4.12, and denies packets sent from all other hosts. This is because the following statement exists at the end of this ACL: **access-list 1 deny any**.

If the ACL contains only the following statement:

```
access-list 1 deny host 192.168.4.12
```

Packets sent from any host will be denied when passing through this port.

When defining an ACL, you must consider the routing update packets. As the implicit "deny all traffic" statement exists at the end of an ACL, all routing update packets may be blocked.

Input Sequence of Rule Statements

Every new rule is added to the end of an ACL and in front of the default rule statement. The input sequence of statements in an ACL is very important. It determines the priority of each statement in the ACL. When determining whether to forward or block packets, a device compares packets with rule statements based on the sequence that rule statements are created. After locating a matched rule statement, the device does not check any other rule statement.

If a rule statement is created and denies all traffic, all subsequent statements will not be checked.

For example:

```
access-list 101 deny ip any any

access-list 101 permit tcp 192.168.12.0 0.0.0.255    eq telnet any
```

The first rule statement denies all IP packets. Therefore, Telnet packets from the host on the network 192.168.12.0/24 will be denied. After the device finds that packets match the first rule statement, it does not check the subsequent rule statements any more.

Related Configuration

Configuring an IP ACL

By default, no IP ACL is configured on a device.

Run the **ip access-list { standard | extended }** {*acl-name* | *acl-id*} command in global configuration mode to create a standard or an extended IP ACL and enter standard or extended IP ACL mode.

Adding ACEs to an IP ACL

By default, a newly created IP ACL contains an implicit ACE that denies all IPv4 packets. This ACE is hidden from users, but takes effect when the ACL is applied to an interface. That is, all IPv4 packets will be discarded. Therefore, if you want the device to receive or send some specific IPv4 packets, add some ACEs to the ACL.

For a standard IP ACL, add ACEs as follows:

- No matter whether the standard IP ACL is a named or number ACL, you can run the following command in standard IP ACL mode to add an ACE:
- [*sn*] { **permit** | **deny** } {**host** *source* | **any** | *source source-wildcard* } [**time-range** *time-range-name*] [**log**]
- For a numbered standard IP ACL, you can also run the following command in global configuration mode to add an ACE:
- **access-list** *acl-id* { **permit** | **deny** } {**host** *source* | **any** | *source source-wildcard* } [**time-range** *tm-rng-name*][**log**]

For an extended IP ACL, you can add ACEs as follows:

Applying an IP ACL

By default, the IP ACL is not applied to any interface, that is, the IP ACL does not filter incoming or outgoing IP packets of the device.

Run the **ip access-group** { ***acl-id*** | ***acl-name*** } { **in**| **out** }command in interface configuration mode to apply a standard or an extended IP ACL to a specified interface.

1.3.2 ACL Logging

ACL logging is used to monitor the running status of ACEs in an ACL and provide essential information for routine network maintenance and optimization.

Working Principle

To better learn the running status of ACLs on a device, you can determine whether to specify the ACL logging option as required when adding ACEs. If this option is specified, logs are output when packets matching ACEs are found. ACL logs are displayed based on ACEs. That is, the device periodically displays ACEs with matched packets and the number of matched packets. An example of the log is as follows:

```
*Sep   9 16:23:06: %ACL-6-MATCH: ACL 100 ACE 10 permit icmp any any, match 78 packets.
```

To control the amount of logs and output frequency, you can configure the log update interval.

An ACE containing the ACL logging option consumes more hardware resources. If all configured ACEs contain this option, the ACE capacity of a device will be reduced by half.

By default, the log update interval is 0, that is, no log is output. After the ACL logging option is specified in an ACE, you need to configure the log update interval to output related logs; otherwise, logs are not output.

For an ACE containing the ACL logging option, if no packet is matched in the specified interval, no packet matching log related to this ACE will be output. If matched packets are found in the specified interval, packet matching logs related to this ACE will be output when the interval expires. The number

of matched packets is the total number of packets that match the ACE during the specified interval, that is, the period from the previous log output to the current log output.

- Only switches support the ACL logging function.
- You can configure the ACL logging option only for an IPv4/IPv6 ACL.

Related Configuration

Configuring an ACL

Configure an ACL before configuring ACEs containing the ACL logging option. For details about how to configure an ACL, see the earlier descriptions about ACL configuration.

Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL and IPv6 ACL. Note that the ACL logging option must be configured.

Configuring the Log Update Interval

Run the {**ip | ipv6** } **access-list log-update inerval** *time* command in the configuration mode to configure the interval at which the ACL logs are output.

Applying an ACL

For details about how to apply an ACL, see the earlier descriptions about the IPv4/IPv6 ACL .

1.3.3 Packet Matching Counters

In addition to ACL logs, packet matching counters provide another choice for routine network maintenance and optimization.

Working Principle

To implement network management, users may want to know whether an ACE has any matched packets and how many packets are matched. ACLs provide the ACE-based packet matching counters. You can enable or disable packet matching counters for all ACEs in an ACL. When a packet matches the ACE, the corresponding counter increments by 1. You can run the **clear counters access-list** [*acl-id* | *acl-name*] command to reset counters of all ACEs in an ACL for a new round of statistics.

- Enabling ACL counters requires more hardware entries. In an extreme case, this will reduce by half the number of ACEs that can be configured on a device.
- You can enable packet matching counters on an IP ACL.
- Only switches support the ACL packet matching counters.

Related Configuration

Configuring an ACL

Configure an ACL before configuring ACEs containing the ACL logging option. For details about how to configure an ACL, see the earlier descriptions about ACL configuration.

Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL and IPv6 ACL. Note that the ACL logging option must be configured.

Enabling Packet Matching Counters

To enable packet matching counters on an IP ACL, run the { **Ip**} **access-list counter** { *acl-id* | *acl-name* } command in global configuration mode.

Applying an ACL

For details about how to apply an ACL, see the earlier descriptions about the IP ACL

Clearing Packet Matching Counters

Run the **clear counters access-list** [*acl-id* | *acl-name*] command in privileged EXEC mode to reset packet matching counters.

1.4 Configuration

Configuration Item	Description and Command	
Configuring an IP ACL	(Optional) It is used to filter IPv4 packets.	
	ip access-list standard	Configures a standard IP ACL.
	ip access-list extended	Configures an extended IP ACL.
	permit host any time-range log	Adds a permit ACE to a standard IP ACL.
	deny host any time-range log	Adds a deny ACE to a standard IP ACL.
	permit host any host any precedence time-range log	Adds a permit ACE to an extended IP ACL.
	deny host any host any precedence time-range log	Adds a deny ACE to an extended IP ACL.
	ip access-group in out	Applies a standard or an extended IP ACL.
Configuring an IPv6 Extended ACL	(Optional) It is used to filter IPv6 packets.	
	ipv6 access-list	Configures an IPv6 ACL.
	permit host any host any range dscp flow-label fragment time-range log	Adds a permit ACE to an IPv6 ACL.
	deny host any host any range dscp flow-label fragment time-range log	Adds a deny ACE to an IPv6 ACL.
	ipv6 traffic-filter in out	Applies an IPv6 ACL.
Configuring Comments for ACLs	(Optional) It is used to configure comments for an ACL or ACE so that users can easily identify the functions of the ACL or ACE.	
	list-remark	Configures a comment for an ACL in ACL configuration mode.

Configuration Item	Description and Command	
	access-list list-remark	Configures a comment for an ACL in global configuration mode.
	remark	Configures a comment for an ACE in ACL configuration mode.

1.4.1 Configuring an IP ACL

Configuration Effect

Configure and apply an IP ACL to an interface to control all incoming and outgoing IPv4 packets of this interface. You can permit or deny the entry of specific IPv4 packets to a network to control access of IP users to network resources.

Notes

N/A

Configuration Steps

Configuring an IP ACL

- (Mandatory) Configure an IP ACL if you want to control access of IPv4 users to network resources.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The IP ACL takes effect only on the local device, and does not affect other devices on the network.

Adding ACEs to an IP ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured, all incoming IPv4 packets of the device are denied by default.

Applying an IP ACL

- (Mandatory) Apply an IP ACL to a specified interface if you want this ACL take effect.
- You can apply an IP ACL on a specified interface of an access, an aggregate, or a core device based on the distribution of users.

Verification

- Use the following methods to verify the configuration effects of the IP ACL:
- Run the **ping** command to verify that the IP ACL takes effect on the specified interface. For example, if an IP ACL is configured to prohibit a host with a specified IP address or hosts in a specified IP address range from accessing the network, run the **ping** command to verify that the host(s) cannot be successfully pinged.
- Access related network resources to verify that the IP ACL takes effect on the specified interface. For example, access the Internet or access the FTP resources on the network through FTP.

Related Commands

Configuring an IP ACL

Command	**ip access-list** { **standard** | **extended** } {*acl-name* | *acl-id* }
Parameter Description	**standard**: Indicates that a standard IP ACL is created. **extended**: Indicates that an extended IP ACL is created. *acl-name*: Indicates the name of a standard or an extended IP ACL. If this option is configured, a named ACL is created. The name is a string of 1 to 99 characters. The ACL name cannot start with numbers (0–9), "in", or "out". *acl-id*: Indicates the ID that uniquely identifies a standard or extended IP ACL. If this option is configured, a numbered ACL is created. If a standard IP ACL is created, the value range of *acl-id* is 1–99 and 1300–1999. If an extended IP ACL is created, the value range of *acl-id* is 100–199 and 2000–2699.
Command Mode	Configuration mode
Usage Guide	Run this command to configure a standard or an extended IP ACL and enter standard or extended IP ACL configuration mode. If you want to control access of users to network resources by checking the source IP address of each packet, configure a standard IP ACL. If you want to control access of users to network resources by checking the source or destination IP address, protocol number, and TCP/UDP source or destination port, configure an extended IP ACL.

Adding ACEs to an IP ACL

- Add ACEs to a standard IP ACL.

Use either of the following methods to add ACEs to a standard IP ACL:

Command	[*sn*] { **permit** | **deny** } {**host** *source* | **any** | *source source-wildcard* } [**time-range** *time-range-name*] [**log**]
Parameter Description	*sn*: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. **host** *source*: Indicates that IP packets sent from a host with the specified source IP address are filtered. **any**: Indicates that IP packets sent from any host are filtered. *source source-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.

	log: Indicates that logs will be periodically output if packets matching the ACEs are found. For details about logs, see "ACL Logging" in this document.
Command Mode	Standard IP ACL configuration mode
Usage Guide	Run this command to add ACEs in standard IP ACL configuration mode. The ACL can be a named or numbered ACL.

Command	**access-list** *acl-id* { **permit** | **deny** } {**host** *source* | **any** | *source source-wildcard* } [**time-range** *tm-rng-name*] [**log**]
Parameter Description	*acl-id*: Indicates the ID of a numbered ACL. It uniquely identifies an ACL. The value range of *acl-id* is 100–199 and 1300–1999. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. **host** *source*: Indicates that IP packets sent from a host with the specified source IP address are filtered. **any**: Indicates that IP packets sent from any host are filtered. *source source-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range. **log**: Indicates that logs will be periodically output if packets matching the ACEs are found. For details about logs, see "ACL Logging" in this document.
Command Mode	Standard IP ACL configuration mode
Usage Guide	Run this command to add ACEs to a numbered IP ACL in global configuration mode. It cannot be used to add ACEs to a named IP ACL.

- Add ACEs to an extended IP ACL.

Use either of the following methods to add ACEs to an extended IP ACL:

Command	[*sn*] { **permit** | **deny** } *protocol* {**host** *source* | **any** | *source source-wildcard* } {**host** *destination* | **any** | *destination destination-wildcard* } [[**precedence** *precedence* [**tos** *tos*]] | **dscp** *dscp*] [**fragment**] [**time-range** *time-range-name*] [**log**]
Parameter Description	*sn*: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE.

	protocol: Indicates the IP protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations to replace the specific IP protocol numbers, including eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp, and udp. **host** *source*: Indicates that IP packets sent from a host with the specified source IP address are filtered. *source source-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **host** *destination:* Indicates that IP packets sent to a host with the specified destination IP address are filtered. If the **any** keyword is configured, IP packets sent to any host are filtered. *destination destination-wildcard:* Indicates that IP packets sent to hosts in a specified IP network segment are filtered. **any**: Indicates that IP packets sent to or from any host are filtered. **precedence** *precedence:* Indicates that IP packets with the specified precedence field in the header are filtered. **tos** *tos:* Indicates that IP packets with the specified the type of service (TOS) field in the header are filtered. **dscp** *dscp*: Indicates that IP packets with the specified the dcsp field in the header are filtered. **fragment:** Indicates that only fragmented IP packets except the first fragments are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range. **log**: Indicates that logs will be periodically output if packets matching the ACEs are found. For details about logs, see "ACL Logging" in this document.
Command Mode	Extended IP ACL configuration mode
Usage Guide	Run this command to add ACEs in extended IP ACL configuration mode. The ACL can be a named or numbered ACL.

Command	**access-list** *acl-id* { **permit** | **deny** } {**host** *source* | **any** | *source source-wildcard* } [**time-range** *time-range-name*] [**log**]
Parameter Description	*acl-id*: Indicates the ID of a numbered ACL. It uniquely identifies an ACL. The value range of *acl-id* is 100–199 and 2000–1999. *sn*: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE.

	protocol: Indicates the IP protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations to replace the specific IP protocol numbers, including eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp, and udp. **host** *source*: Indicates that IP packets sent from a host with the specified source IP address are filtered. *source source-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **host** *destination:* Indicates that IP packets sent to a host with the specified destination IP address are filtered. If the **any** keyword is configured, IP packets sent to any host are filtered. *destination destination-wildcard:* Indicates that IP packets sent to hosts in a specified IP network segment are filtered. **any**: Indicates that IP packets sent to or from any host are filtered. **precedence** *precedence:* Indicates that IP packets with the specified precedence field in the header are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range. **log**: Indicates that logs will be periodically output if packets matching the ACEs are found. For details about logs, see "ACL Logging" in this document.
Command Mode	Extended IP ACL configuration mode
Usage Guide	Run this command to add ACEs to a numbered IP ACL in extended IP ACL configuration mode. It cannot be used to add ACEs to a named extended IP ACL.

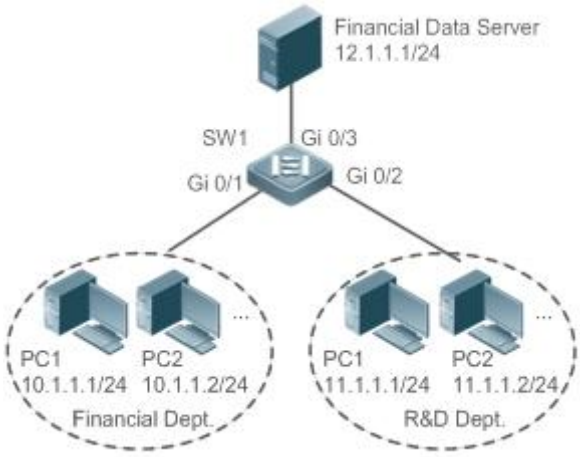
Applying an IP ACL

Command	**ip access-group** { *acl-id* | *acl-name* } { **in** | **out** }
Parameter Description	*acl-id*: Indicates that a numbered standard or extended IP ACL will be applied to the interface. *acl-name*: Indicates that a named standard or extended IP ACL will be applied to the interface. **in**: Indicates that this ACL controls incoming IP packets of the interface. **out**: Indicates that this ACL controls outgoing IP packets of the interface.
Command Mode	Interface configuration mode
Usage Guide	This command makes an IP ACL take effect on the incoming or outgoing packets of a specified interface

Configuration Example

The following configuration example describes only ACL-related configurations.

Configuring an IP ACL to Prohibit Departments Except the Financial Department from Accessing the Financial Data Server

Scenario Figure 1-3	
Configuration Steps	● Configure an IP ACL. ● Add ACEs to the IP ACL. ● Apply the IP ACL to the outgoing direction of the interface connecting the financial data server.
SW1	sw1(config)#ip access-list standard 1 sw1(config-std-nacl)#permit 10.1.1.0 0.0.0.255 sw1(config-std-nacl)#deny 11.1.1.1 0.0.0.255 sw1(config-std-nacl)#exit sw1(config)#int gigabitEthernet 0/3 sw1(config-if-GigabitEthernet 0/3)#ip access-group 1 out
Verification	● On a PC of the R&D department, ping the financial data server. Verify that the ping operation fails. ● On a PC of the financial department, ping the financial data server. Verify that the ping operation succeeds.
SW1	sw1(config)#show access-lists ip access-list standard 1 10 permit 10.1.1.0 0.0.0.255 20 deny 11.1.1.0 0.0.0.255 sw1(config)#show access-group ip access-group 1 out Applied On interface GigabitEthernet 0/3

1.4.2 Configuring the Time Range-Based ACEs

Configuration Effect

Configure the time range-based ACEs if you want some ACEs to take effect or to become invalid in a specified period of time, for example, in some time ranges during a week.

Configuration Steps

Configuring an ACL

- (Mandatory) Configure an ACL if you want ACEs to take effect in the specified time range. For details about the configuration method, see the earlier descriptions.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The configurations take effect only on the local device, and do not affect other devices on the network.

Adding an ACE with the Time Range Specified

- (Mandatory) Specify the time range when adding an ACE. For details about how to configure the time range, see the configuration manual related to the time range.

Applying an ACL

- (Mandatory) Apply the ACL to a specified interface if you want to make ACEs take effect in the specified time range.
- You can apply an IP ACL on a specified interface of an access, an aggregate, or a core device based on the distribution of users.

Verification

In the time range that the configured ACE takes effect or becomes invalid, run the **ping** command or construct packets matching the ACE to check whether the ACE takes effect or becomes invalid.

Related Commands

Configuring an ACL

For details about the ACL configuration commands, see the earlier descriptions about the IPv4/IPv6 ACL.

Adding an ACE with the Time Range Specified

For details about the ACE configuration commands, see the earlier descriptions about the IPv4/IPv6 ACL.

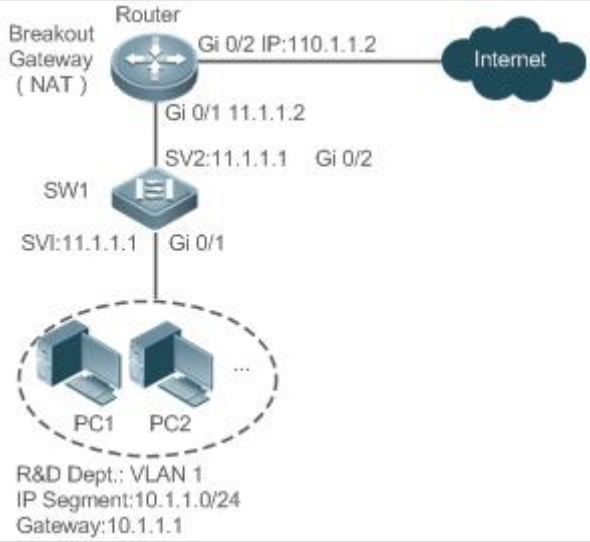
Applying an ACL

For details about the command for applying an ACL, see the earlier descriptions about the IPv4/IPv6 ACL.

Configuration Example

The following configuration example describes only ACL-related configurations.

Adding an ACE With the Time Range Specified to Allow the R&D Department to Access the Internet Between 12:00 and 13:30 Every Day

Scenario Figure 1-4	
Configuration Steps	● Configure a time range named "access-internet", and add an entry of the time range between 12:00 and 13:30 every day. ● Configure an IP ACL "ip_std_internet_acl". ● Add an ACE to allow packets with the source IP address in the network segment 10.1.1.0/24, and associate this ACE with the time zone "access-internet". ● Add an ACE to deny packets with the source IP address the network segment 10.1.1.0/24. Access to the Internet is not allowed except in the specified time range. ● Add an ACE to permit all packets. ● Apply the ACL to the outgoing direction of the interface connected to the breakout gateway.
SW1	FS(config)# time-range access-internet FS(config-time-range)# periodic daily 12:00 to 13:30 FS(config-time-range)# exit sw1(config)# ip access-list standard ip_std_internet_acl sw1(config-std-nacl)# permit 10.1.1.0 0.0.0.255 time-range access-internet sw1(config-std-nacl)# deny 10.1.1.0 0.0.0.255 sw1(config-std-nacl)# permit any sw1(config-std-nacl)# exit sw1(config)#int gigabitEthernet 0/2 sw1(config-if-GigabitEthernet 0/2)# ip access-group ip_std_internet_acl out
Verification	● Within the time range between 12:00 and 13:30, visit the Baidu website on a PC of the R&D department. Verify that the website can be opened normally. ● Beyond the time range between 12:00 and 13:30, visit the Baidu website on a PC of the

	R&D department. Verify that the website cannot be opened.
SW1	sw1#show time-range time-range entry: access-internet (inactive) periodic Daily 12:00 to 13:30 sw1#show access-lists ip access-list standard ip_std_internet_acl 10 permit 10.1.1.0 0.0.0.255 time-range access-internet (inactive) 20 deny 10.1.1.0 0.0.0.255 30 permit any sw1#show access-group ip access-group ip_std_internet_acl out Applied On interface GigabitEthernet 0/2

1.4.3 Configuring Comments for ACLs

Configuration Effect

During network maintenance, if a lot of ACLs are configured without any comments, it is difficult to distinguish these ACLs later on. You can configure comments for ACLs to better understand the intended use of ACLs.

Configuration Steps

Configuring an ACL

- (Mandatory) Configure an ACL before configuring the security channel. For details about the configuration method, see the earlier descriptions.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The configurations take effect only on the local device, and do not affect other devices on the network.

Configuring Comments for ACLs

- (Optional) Configure comments for ACLs so that it is easy to manage and understand the configured ACLs.

Adding ACEs to an ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured, it is equivalent that the security channel does not take effect. For details about how to add an ACE to an ACL, see the related descriptions.

Configuring Comments for ACEs

- (Optional) To facilitate understanding of a configured ACL, you can configure comments for ACEs in addition to comments for the ACL.

Verification

Run the **show access-lists** command on the device to display the comments configured for ACLs.

Related Commands

Configuring an ACL

For details about how to configure an ACL, see the earlier descriptions about the IPv4/IPv6 ACL.

Configuring a Comment for an ACL

Use either of the following two methods to configure a comment for an ACL:

Command	**list-remark** *comment*
Parameter Description	***comment***: Indicates the comment. The value is a string of 1 to 100 characters. A comment longer than 100 characters will be truncated to 100 characters.
Command Mode	ACL configuration mode
Usage Guide	Run this command to configure the comment for a specified ACL.

Command	**access-list** *acl-id* **list-remark** *comment*
Parameter Description	***acl-id***: Indicates the ID of an ACL. ***comment***: Indicates the comment. The value is a string of 1 to 100 characters. A comment longer than 100 characters will be truncated to 100 characters.
Command Mode	Configuration mode
Usage Guide	Run this command to configure the comment for a specified ACL.

Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IPv4/IPv6 ACL.

Configuring Comments for ACEs

Use either of the following two methods to configure a comment for an ACE:

Command	**remark** *comment*
Parameter	***comment***: Indicates the comment. The value is a string of 1 to 100 characters. A comment

Description	longer than 100 characters will be truncated to 100 characters.
Command Mode	ACL configuration mode
Usage Guide	Run this command to configure the comment for a specified ACE.

Command	**access-list** *acl-id* **remark** *comment*
Parameter Description	***acl-id***: Indicates the ID of an ACL. ***comment***: Indicates the comment. The value is a string of 1 to 100 characters. A comment longer than 100 characters will be truncated to 100 characters.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure the comment for a specified ACE.

1.5 Monitoring

Clearing

Description	Command
Clears the ACL packet matching counters.	**clear counters access-list** [*acl-id* | *acl-name*]
Clears the counters of packets matching the deny ACEs.	**clear access-list counters** [*acl-id* /*acl-name*]

Displaying

Description	Command
Displays the basic ACLs.	**show access-lists** [*acl-id* | *acl-ame*] [**summary**]
Displays the ACL configurations applied to an interface.	**show access-group** [**interface** *interface-name*]
Displays the IP ACL configurations applied to an interface.	**show ip access-group** [**interface** *interface-name*]
Displays the IPv6 ACL configurations applied to an interface.	**show ipv6 traffic-filter** [**interface** *interface-name*]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the ACL running process.	**debug acl acld event**
Debugs the ACL clients.	**debug acl acld client-show**
Debugs the ACLs created by all ACL clients.	**debug acl acld acl-show**

2 Configuring RPL

2.1 Overview

Reverse Path Limit (RPL) enables packets to be sent and returned along the same path, ensuring that these packets are not discarded by firewalls that do not allow one-way connection.

When creating a flow entry, a router buffers packet data according to the number of the inbound port receiving the first packet. Reply packets of the same data flow are matched to the flow entry preferentially and are forwarded through the inbound port. (Both the routing table and policy-based routing [PBR] table are not used.)

FS gateway devices are equipped with the RPL module to ensure data flow access security.

RPL is applicable to access with sticky load balancing at network egresses.

2.2 Applications

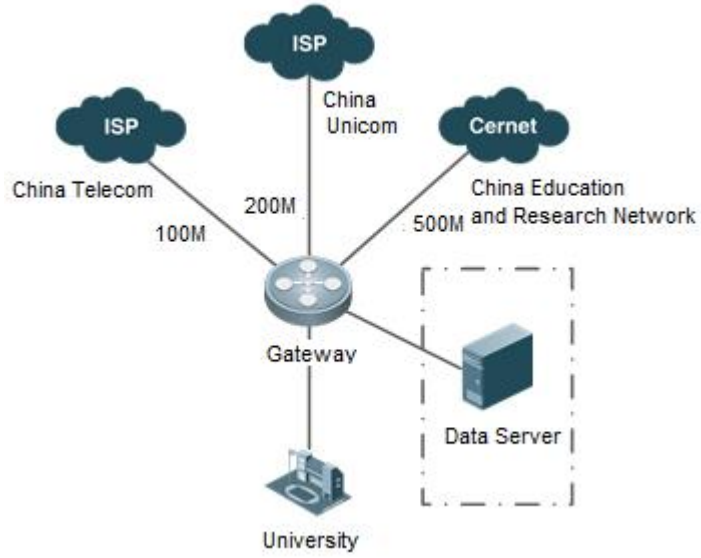
Application	Description
Send and Return Data Flows Along the Same Path	The data server of a university returns reply packets along the same path where external data requests are sent.

2.2.1 Send and Return Data Flows Along the Same Path

Scenario

- RPL is enabled on interfaces which require data flows to be sent and returned along the same path.

Figure 2-1



Deployment

- Enable the RPL module on interfaces.

2.3 Features

Basic Concepts

Flow

A flow or streaming session consists of packets sent during a period and with the same quintuple (source IP address, source port, destination IP address, destination port, and protocol).

A flow contains two directions: forward and reverse. The direction how the initial packet travels to an end device is defined as “forward”, and the opposite direction as “reverse”. For example, an intranet initiates a request to access resources in an extranet and the extranet responses, so the forward direction is from LAN port to WAN port and the reverse is from WAN port to LAN port. However, if the extranet initiates a request to access resources in the intranet, then the forward direction is from WAN port to LAN port while the reverse is from LAN port to WAN port.

Working Principle

After RPL is enabled on an interface, when the interface receives a forward flow, its source interface and source MAC address are recorded. Then, when a reverse flow reaches the end device, based on the record, the target interface of the reverse flow is changed to the source interface of the forward flow and the target MAC address to the source MAC address. In this way, the routing table is not used.

RPL cannot distinguish between a LAN port and a WAN port. If VRRP is applied on the peer end, the source MAC address may be a virtual MAC address, which leads to a wrong next hop. Therefore, RPL is not supported in the VRRP scenario.

Overview

Feature	Description
RPL Switch	Enables and disables the RPL module.

2.3.1 RPL Switch

The RPL switch is used to enable and disable the RPL module.

Working Principle

After the RPL module is enabled, data flows are sent and returned along the same path.

After the RPL module is disabled, data flows are not necessarily sent and returned along the same path.

Related Configuration

Enabling the RPL Module

By default, the RPL module is disabled on the interfaces on FS gateway devices.

To enable the RPL module, run the **reverse-path** command in interface configuration mode.

Disabling the RPL Module

By default, the RPL module is disabled on the interfaces on FS gateway devices.

To disable the RPL module on interfaces, run the **no reverse-path** command in interface configuration mode.

2.4 Configuration

Configuration	Description and Command	
Enabling RPL	(Mandatory) It is used to enable RPL.	
	reverse-path	Enables the RPL module in interface configuration mode.

2.4.1 Enabling RPL

Configuration Effect

Enable RPL in interface configuration mode to allow data flows to be sent and returned along the same path.

Notes

- The interfaces which require data flows to be sent and returned along the same path must be able to find the corresponding route (that is, the outbound route and next-hop IP address can be displayed by running the **show ip route** command).

Configuration Steps

Enabling the RPL Module

- Mandatory.

Related Commands

Enabling the RPL Module

Command	**reverse-path**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Enabling RPL

Scenario	N/A
Configuration Steps	• Enable RPL in interface configuration mode. FS(config-if-GigabitEthernet 0/1)# reverse-path
Verification	Display interface configurations. • Run the **show running-config interface gigabitEthernet 0/1** command to display

	interface configurations. FS(config)# show running-config interface gigabitEthernet 0/1 Building configuration... Current configuration : 73 bytes ! interface GigabitEthernet 0/1 duplex auto speed auto reverse-path

2.5 Monitoring

N/A

3 Configuring RNFP

3.1 Overview

FS Network Foundation Protection (RNFP) is a collection of means for defending devices against attacks.

When encountering network attacks or high loads, RNFP is capable of protecting key resources on the control and management plane of routers, to prevent device breakdown and improve device availability.

3.2 Applications

Application	Description
There Are a Large Amount of Traffic that Attacks Devices on the Network	A large amount of abnormal traffic on the network will cause very high CPU utilization of devices, slow or suspended response of the Command Line Interface (CLI), loss of link or network control protocol packets, and finally link or network jitter. The processing bandwidth is occupied by illegitimate packets, which results in the failure to process important protocol packets.

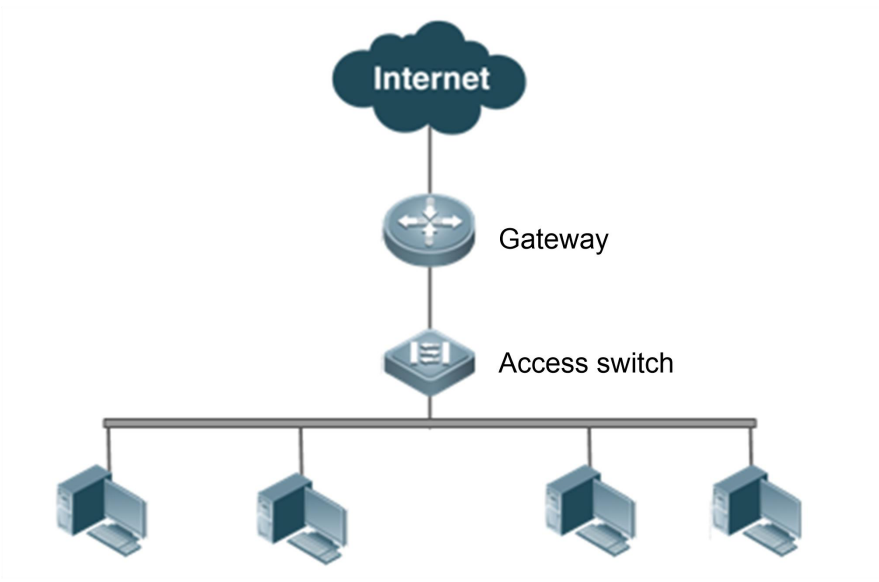
3.2.1 There Are a Large Amount of Traffic that Attacks Devices on the Network

Scenario

In the network-attacked environment, RNFP reduces the CPU utilization in case of attacks and safeguards key protocol packets so that administrators can access the devices normally.

- Restricts attack traffic.
- Safeguards non-attack traffic.

Figure 3-1



Deployment

- Configure the local anti-attack rate-limit policy on the device.
- Add the IP address of the administrator to the whitelist to safeguard the traffic for the administrator to manage devices.

3.3 Features

Basic Concepts

Classify

RNFP identifies and classifies data traffic transmitted to the control plane. It classifies traffic into the protocol traffic, manage traffic, and data traffic, which facilitates submodules to limit the rate and filter traffic in a differentiated manner.

Sub-interface

All traffic transmitted to the control plane is classified by Classify into three types, which are separately processed by the three sub-interfaces below:

- Protocol sub-interface: Processes all protocol control traffic transmitted to the local device, including link-layer protocol packets and routing protocol packets.
- Manage sub-interface: Processes all management protocol traffic transmitted to the local device, such as FTP, Telnet, SNMP, and ARP protocol packets.
- Data sub-interface: Processes all data traffic that cannot be processed by the fast forwarding plane.

SCPP

Segregate Control Plane Protection (SCPP), according to user-defined policies, match traffic of the three sub-interfaces to different ACLs according to user-defined policies, to implement finer-granularity rate limit and protection.

Glean-CAR

Glean-CAR limits the rate of the traffic that is matched by the fast forwarding plane to the REF Glean adjacency (the traffic is matched to the direct route but the host route that matches the destination IP address is not found, and therefore the traffic needs to be transmitted to the control plane for destination IP address resolution).

ARP-CAR

The fast forwarding plane cannot process ARP packets and need to transmit them to the control plane for processing. ARP-CAR can limit the rate of ARP packets for each neighbor.

Port-Filter

Port-Filter checks whether ports are enabled on local applications for TCP and UDP packets transmitted to the local device, and filters out the traffic transmitted to the local device, for which the network service is not enabled on the local device, before the traffic reaches the control plane.

MPP

Management Plane Protection (MPP) allows administrators to specify one or multiple interfaces as the inband management interfaces (supporting receiving of management packets and forwarding of normal services). After MPP is enabled, only a specified inband management interface is allowed to receive management packets of a specified protocol. Service packets, protocol packets, and ARP packets are not affected.

ACPP

Aggregate Control Plane Protection (ACPP) uses the default or user-defined rate to limit the rate of the traffic on the protocol sub-interface, manage sub-interface, and data sub-interface based on classification results of Classify, to ensure that the traffic does not exceed the processing capacity of the control plane, thereby protecting the control plane.

Local Anti-attack Whitelist

When accessing an attacked device, users will feel stuck or fail to access the device. The local anti-attack whitelist can be configured to free whitelisted users from all anti-attack policies, their device access packets are not discarded due to rate limit, thereby preventing stuck access or access failures.

User Management Device Restriction

User management device restriction forbids intranet/extranet users to ping the device, access the Web page of the device, telnet to the device or log in to the device in Secure Shell (SSH) mode, and manage the device over the Simple Network Management Protocol (SNMP), with no need to associate Access Control Lists (ACLs).

ARP Attack Detection

In a Layer-2 environment, the Address Resolution Protocol (ARP) attacks in the intranet may affect the normal Internet access of intranet users. ARP attack detection aims at detecting possible ARP attacks on the network and listing suspicious hosts of ARP attacks for administrators to locate and rectify faults.

Sub-interfaces involved in the device anti-attack are different from traditional sub-interfaces of devices. A device anti-attack interface indicates an internal channel for transmitting a certain type of traffic to the control plane. Such interfaces can be used to conveniently conduct anti-attack configuration and processing on traffic.

Anti-attack sub-functions of devices (SCPP, Glean-CAR, ARP-CAR, Port-Filter, MPP, and ACPP) are independent of each other in the configuration. Users can combine or configure anti-attack sub-functions according to requirements and policies. Note that some sub-interfaces have restrictions on the application sub-interfaces.

Overview

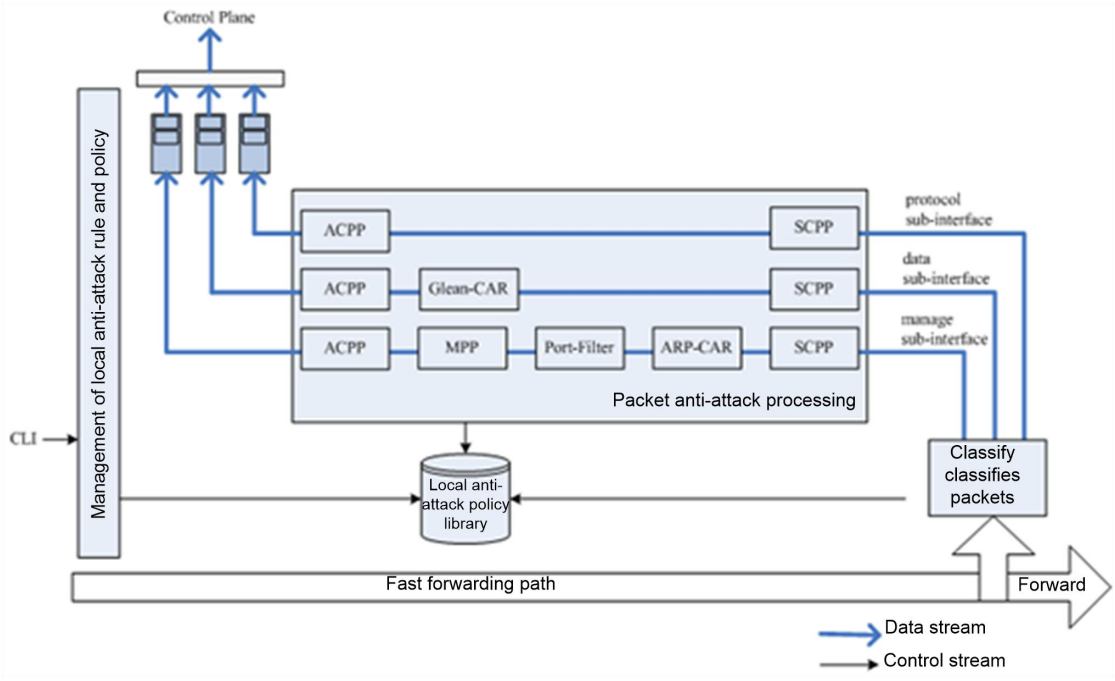
Feature	Description
Local Anti-attack	Distributes packets transmitted to the control plane to different sub-interfaces for rate limit based on the packet type.
Attack Detection	Detects attack behaviors on the network.
Local Anti-attack Whitelist	Ensures management traffic by not limiting the rate of traffic from whitelisted users.

User Management Device Restriction	Forbids intranet/extranet users to ping the device, access the Web page of the device, telnet to the device or log in to the device in SSH mode, and manage the device over SNMP.

3.3.1 Local Anti-attack

Classify and filter data packets to be processed by the control plane, and limit their rates, so as to protect key resources of the control plane.

Working Principle



As shown in the figure above, packet classification and rate limit are implemented by multiple submodules. Packets to be processed by the control plane are classified and then rate limit is conducted on them according to policies configured for different sub-interfaces.

- **protocol sub-interface**

The protocol sub-interface conducts rate limit and filtering on all protocol control traffic transmitted to the local device. It covers two submodules: SCPP and ACPP. Packets are processed by in SCPP > ACPP order.

- **data sub-interface**

The data sub-interface conducts rate limit and filtering on all traffic that cannot be processed by the fast forwarding plane. It covers three submodules: SCPP, Glean-CAR, and ACPP. Packets are processed by in SCPP > Glean-CAR > ACPP order.

- **manage sub-interface**

The manage sub-interface conducts rate limit and filtering on all management protocol traffic transmitted to the local device. It covers five submodules: SCPP ARP-CAR, Port-Filter, MPP, and ACPP. Packets are processed by in SCPP > ARP-CAR > Port-Filter > MPP >ACPP order.

ACPP directly forwards the packets allowed by SCPP, ARP packets, and Glean packets without rate limit.

Related Configuration

Configuring Local Anti-attack

By default, all rate limit functions are disabled.

Run the **control-plane** [**protocol** | **manage** | **data**] command to access different sub-interfaces and configure different function policies for the sub-interfaces.

Run the **ef-rnfp enable** command to globally enable packet classification and rate limit.

Run the **scpp list** *acl_no* { [**bw-rate** *rate* **bw-burst-rate** *brust-rate*] [**conn-create-rate** *create-rate* **conn-create-burst-rate** *create-burst-rate*] [**conn-total** *num*] } [**log**] command to configure SCPP to limit the rate of ACL-matched packets and adjust the rate limit values of SCPP.

Run the **acpp bw-rate** *rate* **bw-burst-rate** *burst-rate* [**log**] command to configure the ACPP rate limit.

Run the **glean-car** *packet_rate_per_group* [**log**] command to configure Glean-CAR and limit the rate of packets that matches the Glean-CAR.

Run the **port-filter** [**log**] command to configure port-filter to reject packets received by locally disabled ports.

Run the **management-interface** *interface* **allow** { **ftp** | **http** | **ssh** | **snmp** | **telnet** | **tftp** } [**log**] command to configure the management interface and configure the management interface to receive packets of the specified management protocols. Non-configured interfaces cannot receive packets of these protocols.

Run the **arp-car** *packet_rate_per_group* [**log**] command to configure ARP-CAR to limit the rate of ARP packets.

3.3.2 Attack Detection

Detect and record attack behaviors on the network.

Working Principle

When the total packets discarded by submodules of sub-interfaces reach a threshold, the device considers that traffic attack occurs on the network. It collects statistics on the type of attack packets, IP addresses, packet count, and packet size.

When the device receives abnormal ARP packets from a host, it records the host as the suspicious host of ARP attacks. The device considers that ARP spoofing occurs and adds the hosts to the ARP spoofing suspect list in the event of the following cases: A host conducts ARP scanning on the entire network (by default, more than 200 ARP requests are transmitted within 10s); the MAC address of a host maps to multiple IP addresses; the MAC address attempted to be updated based on an ARP request is different from the existing MAC address.

Related Configuration

Configuring Traffic Attack Detection

By default, attack detection is disabled. When the **ef-rnfp enable** command is executed to globally enable packet classification and rate limit, traffic attack detection is enabled by default.

Run the **attack threshold** *drop-num* command to set the attack judgment threshold. The default value is 500.

Run the **show attack** { **current** | **history** } command to display attack information.

Configuring ARP Attack Detection

By default, attack detection is disabled.

Run the **anti-arp-spoof** command to enable ARP attack detection.

Run the **anti-arp-spoof** [**scan** *arp-num*] command to set the ARP scanning threshold. The default value is 20.

Run the **show arp-suspect** command to display the ARP spoofing suspect list.

3.3.3 Local Anti-attack Whitelist

Add the IP address of the administrator to the whitelist so that the administrator can normally manage devices even if the network is attacked.

Working Principle

The local anti-attack module does not limit the rate of traffic from whitelisted IP addresses but allows the traffic to directly pass.

Related Configuration

Configuring the Local Anti-attack Whitelist

By default, there is no IP address in the whitelist.

Run the **security web permit** *low-ip-address* [*high-ip-address*] command to configure the whitelist range. A maximum of 32 IP addresses or IP address segments are supported.

3.3.4 User Management Device Restriction

For common Ping, Web, Telnet, SSH, and SNMP attack behaviors on the network, user management device restriction forbids intranet/extranet users to ping the device or access the Web page of the device, with no need to use ACLs, delivering great flexibility and convenience.

Working Principle

User management device restriction intercepts ping packets, Web packets for device access, Telnet packets or SSH login packets, and SNMP packets, in an effort to forbid the ping, Web access, Telnet and SSH login, and SNMP management behaviors.

Related Configuration

Configuring User Management Device Restriction

By default, the function is disabled.

Run the **security deny** { **lan-ping** | **lan-web** | **wan-ping** | **wan-web** | **lan-telnet-ssh** | **lan-snmp** | **wan-telnet-ssh** | **wan-snmp** } command to configure the user management device restriction function.

3.4 Configuration

Configuration	Description and Command	
Configuring Local Anti-attack	(Optional) It is used to configure rate limit rules.	
	control-plane	Enters the control-plane configuration mode.
	scpp	Configures SCPP.
	glean-car	Configures Glean rate limit.
	arp-car	Configures ARP rate limit.
	port-filter	Configures port filtering.
	mpp	Configures MPP.
	acpp	Configures ACPP.
	ef-rnfp	Enables local anti-attack.
Configuring Attack Detection	(Optional) It is used to configure attack detection rules.	
	attack threshold	Configures the attack confirmation threshold.
	anti-arp-spoof	Configures ARP attack detection.
Configuring the Local Anti-attack Whitelist	(Optional) It is used to configure local anti-attack whitelisted users.	
	security web permit	Configures whitelisted IP addresses.
Configuring User Management Device Restriction	(Optional) It is used to forbid intranet/extranet users to ping the device, access the Web page of the device, telnet to the device or log in to the device in SSH mode, and manage the device over SNMP.	
	security deny	Forbids intranet/extranet users to ping the device, access the Web page of the device, telnet to the device or log in to the device in SSH mode, and manage the device over SNMP.

3.4.1 Configuring Local Anti-attack

Configuration Effect

- Reduce the CPU utilization of the device even if the network is attacked.
- Improve the CLI response speed even if the network is attacked.
- Safeguard important packets such as link or network control protocol packets when the network is attacked.

Notes

- If the Telnet operation and Web access slow down after the function is configured, you can add the IP address used in the Telnet operation and Web access to the local anti-attack whitelist to ensure the traffic of the IP address.

Configuration Steps

Entering the control-plane Configuration Mode

- Mandatory.
- Enter different sub-interfaces.

Configuring Rate Limit

- Mandatory.
- Configure different functions to implement rate limit.

Verification

- Check the CPU utilization.
- Check the CLI response speed.
- Check whether important protocol packets are safeguarded.

Related Commands

Entering the control-plane Configuration Mode

Command	**control-plane** [**protocol** | **manage** | **data**]
Parameter Description	**protocol**: Enters the protocol sub-interface. **manage**: Enters the manage sub-interface. **data**: Enters the data sub-interface. Non-sub-interface functions are configured if no parameter is set.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring SCPP

Command	**scpp list** *acl_no* { [**bw-rate** *rate* **bw-burst-rate** *burst-rate*] [**conn-create-rate** *create-rate* **conn-create-burst-rate** *create-burst-rate*] [**conn-total** *num*] } [**log**]
Parameter Description	**list** *acl_no*: Indicates ACL rules, which are used to search out the traffic to be processed by SCPP. **bw-rate** *rate*: Indicates the rate limit. The unit is pps. **bw-burst-rate** *burst-rate*: Indicates the burst rate limit. The unit is pps. **conn-create-rate** *create-rate*: Indicates the rate limit for connection creation per second. **conn-create-burst-rate** *create-burst-rate*: Indicates the rate limit for burst connection creation per second. **conn-total** *num*: Indicates the limit on the total number of connections. **log**: Indicates whether to output logs.
Command Mode	control-plane mode
Usage Guide	The three sub-interfaces can conduct SCPP processing on traffic on the sub-interfaces. By default, SCPP is disabled. It is enabled only after users explicitly configure SCPP rules.

Configuring Glean Rate Limit

Command	**glean-car** *packet_rate_per_group*
Parameter Description	*packet_rate_per_group*: Configures the rate limit value for the traffic that is initiated by users (sources), who are in the same group according to the hash algorithm, and is matched to the Glean adjacency. The unit is pps.
Command Mode	control-plane mode
Usage Guide	The Glean-CAR function can be configured only on the data sub-interface. Currently, the hash algorithm extracts lower *N* bits from the source address (the value of *N* varies with products). Note that Glean-CAR can limit the rate of the traffic that is initiated by users, who are in the same group according to the hash algorithm, and is matched to the Glean adjacency. For example, User A (with IP address of 192.168.52.57) and User B (with IP address of 192.168.60.57) (share the same hash result) send traffic to directly connected Destination Host C (with IP address of 172.16.0.5). Before 172.16.0.5 is successfully resolved by ARP, if Glean-CAR 5 is configured, a maximum of five packets out of the traffic initiated by User A and User B can be transmitted to the control plane every second, requesting the control plane to conduct ARP resolution on the destination IP address. By default, Glean-CAR is disabled. It is enabled only after users explicitly configure Glean-CAR rules.

Configuring ARP Rate Limit

Command	**arp-car** *packet_rate_per_group*
Parameter Description	*packet_rate_per_group*: Configures the rate limit value for ARP traffic that is initiated by users, who are in the same group according to the hash algorithm. The unit is pps.
Command Mode	control-plane mode
Usage Guide	The ARP-CAR function can be configured only on the manage sub-interface. Currently, the hash algorithm extracts lower *N* bits from the source address (the value of *N* varies with products). Note that ARP-CAR can limit the rate of the ARP traffic initiated by users who are in the same group according to the hash algorithm. For example, User A (with IP address of 192.168.52.57) and User B (with IP address of 192.168.60.57) (share the same hash result) send the ARP request for 192.168.52.1 to the device. If ARP-CAR 5 is configured, a maximum of five packets out of the traffic initiated by User A and User B can be transmitted to the control plane every second, requesting the control plane to give ARP response. By default, ARP-CAR is disabled. It is enabled only after users explicitly configure ARP-CAR rules.

Configuring Port Filtering

Command	**port-filter**
Parameter Description	N/A

Command Mode	control-plane mode
Usage Guide	Configure Port-Filter to filter out received transport-layer packets, for which services are not enabled. The Port-Filter function can be configured only on the manage sub-interface. By default, Port-Filter is disabled. It is enabled only after users explicitly configure Port-Filter.

Configuring MPP

Command	**management-interface** *interface* **allow** { **ftp** | **http** | **ssh** | **snmp** | **telnet** | **tftp** }
Parameter Description	*interface*: Specifies an inband management interface. **allow** { **ftp** | **http** | **ssh** | **snmp** | **telnet** | **tftp** }: Configures the allowed management protocol.
Command Mode	control-plane mode
Usage Guide	Configure MPP to specify an inband management interface and management protocol packets allowed by the interface. The MPP sub-function can be configured only on the manage sub-interface. A maximum of 16 inband management interfaces can be configured, and each interface can receive packets of multiple or all management protocols. After MPP is enabled, non-inband management interfaces are not allowed to receive management packets, and inband management interfaces are allowed to receive packets of only specified management protocols. By default, MPP is disabled. It is enabled only after users explicitly configure MPP rules.

Configuring ACPP

Command	**acpp bw-rate** *rate* **bw-burst-rate** *burst-rate*
Parameter Description	*rate*: Indicates rate limit. The unit is pps. *burst-rate*: Indicates burst rate limit. The unit is pps.
Command Mode	control-plane mode
Usage Guide	Configure ACPP for classified traffic that is transmitted to the control plane. The three sub-interfaces can conduct ACPP processing on the traffic on the sub-interfaces. By default, ACPP is disabled. It is enabled only after users explicitly configure ACPP rules.

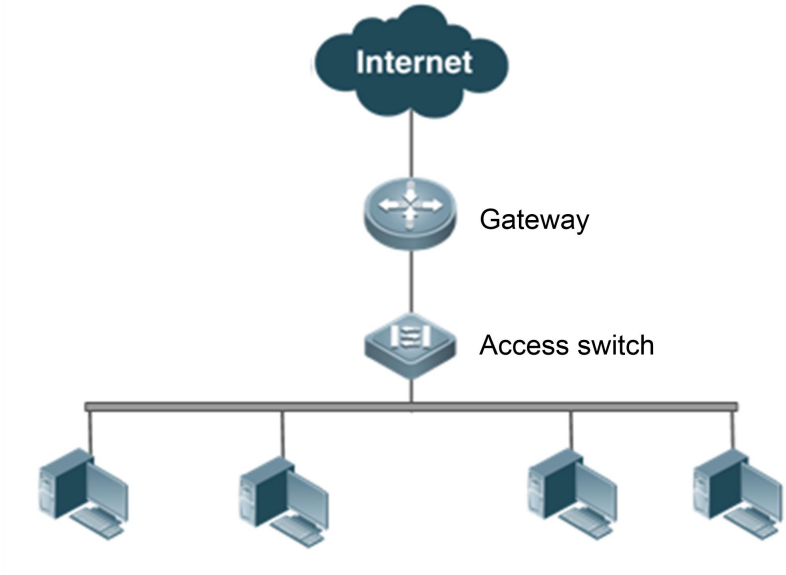
Enabling Local Anti-attack

Command	**ef-rnfp** { **enable** | **disable** }
Parameter Description	**enable**: Enables local anti-attack. **disable**: Disables local anti-attack.
Command Mode	control-plane mode
Usage Guide	When no local anti-attack policy is configured, if local anti-attack is enabled, the default policy (ACPP on each sub-interface, port-filter on the manage sub-interface, and Glean-CAR on the data sub-interface) is enabled. The default anti-attack rules and policy are set based

	on different products and platforms. After local anti-attack is disabled, rate limit functions are all unavailable.

Configuration Example

Configuring Local Anti-attack on the Gateway

Scenario Figure 3-2	
Configuration Steps	● Configure the local anti-attack rate-limit policy on the gateway. ● Configure ACPP on the protocol sub-interface, and set the rate limit to 500 pps for the traffic on the protocol sub-interface and allowable burst peak to 600 pps. ● Configure ACPP on the data sub-interface, and set the rate limit to 500 pps for the traffic on the data sub-interface and allowable burst peak to 600 pps. ● Configure Glean-CAR to allow 10 packets from each source to be matched to the Glean adjacency every second. ● Configure ACPP on the manage sub-interface, and set the rate limit to 500 pps for the traffic on the manage sub-interface and allowable burst peak to 600 pps. ● Configure ARP-CAR to allow 10 ARP packets from each source to pass every second. ● Configure Port-Filter. ● Configure MPP rules, in which Port Gi0/0 is specified as the inband management interface, and the interface is allowed to receive packets of only the Telnet and SNMP protocols. ● Enable local anti-attack globally.
A	FS # configure terminal FS(config)# control-plane protocol FS(config-cp)# acpp bw-rate 500 bw-burst-rate 600 FS(config)# control-plane data FS(config-cp)# acpp bw-rate 500 bw-burst-rate 600

	FS(config-cp)# glean-car 10 FS(config)# control-plane manage FS(config-cp)# acpp bw-rate 500 bw-burst-rate 600 FS(config-cp)# arp-car 10 FS(config-cp)# port-filter FS(config-cp)# management-interface gi0/0 allow telnet snmp FS(config)# control-plane FS(config-cp)# ef-rnfp enable
Verification	Run the **show ef-rnfp alll** command to display the configuration.

A	FS# show ef-rnfp all
	Aggregate control plane protection information:
	  Data subinterface: enable
	  RULE:
	  bandwidth rate limit: 500(pps), burst: 600(pps)
	  log: off
	  STATISTIC:
	  dropped 0 packets
	  Manage subinterface: enable
	  RULE:
	  bandwidth rate limit: 500(pps), burst: 600(pps)
	  log: off
	  STATISTIC:
	  dropped 0 packets
	  Protocol subinterface: enable
	  RULE:
	  bandwidth rate limit: 500(pps), burst: 600(pps)
	  log: off
	  STATISTIC:
	  dropped 0 packets
	Segregate control plane protection information:
	  Data subinterface: disable
	  Manage subinterface: disable
	  Protocol subinterface: disable

```
ARP CAR information:
  Manage subinterface:  enable
    RULE:
      allow packet rate per source:  10(pps)
      log:  off
    STATISTIC:
      dropped 0 packets
Glean CAR information:
  Data subinterface:  enable
    RULE:
      allow packet rate per source:  10(pps)
      log:  off
    STATISTIC:
      dropped 0 packets
Port Filter information:
  Manage subinterface:  enable
    RULE:
      TCP open port:
        23, 80, 1723, 2650, 4430, 8081,
      UDP open port:
        67, 68, 161, 514, 3784, 3785, 6000,
        log:  off
    STATISTIC:
      dropped 0 tcp packets
      dropped 0 udp packets
Management plane protection information:
  Manage subinterface:  enable
    RULE:  management interface:  GigabitEthernet 0/0, id:  1fa52
      allow:    snmp telnet
      log:  off
    STATISTIC:
      dropped 0 disallow management protocol packets
  dropped 0 management protocol packet from non management interface
```

Common Errors

- If only an interface is configured as the inband management interface, other interfaces may not be managed normally.

3.4.2 Configuring Attack Detection

Configuration Effect

- The device can detect and record attacks occurring on the network.

Notes

- The local anti-attack must be enabled.

Configuration Steps

Entering the Global control-plane Mode

- Mandatory.

Configuring the Traffic Attack Detection Threshold

- Mandatory.
- Configure the traffic attack detection threshold.

Configuring ARP Attack Detection

- Mandatory.
- Configure the ARP attack detection policy.

Verification

- The device can detect traffic attacks on the network.
- The device can detect ARP attacks on the network.

Related Commands

Configuring the Attack Confirmation Threshold

Command	**attack threshold** *drop-num*
Parameter Description	*drop-num*: Indicates the rate threshold of packets discarded by the local anti-attack module for determining whether network attacks exist. The unit is pps.
Command Mode	control-plane mode
Usage Guide	N/A

Configuring ARP Attack detection

Command	**anti-arp-spoof** [**scan** *arp-num*]
Parameter Description	*arp-num*: Indicates the quantity threshold of ARP packets received from an IP address per second within 10 seconds for determining whether the IP address is used to conduct ARP scanning.

	ARP attack detection is enabled if no parameter is set.
Command Mode	control-plane mode
Usage Guide	Enable ARP anti-attack. If this command is run, the device is capable of identifying ARP spoofing. It considers that ARP spoofing occurs and adds the hosts to the ARP spoofing suspect list in the event of the following cases: A host conducts ARP scanning on the entire network (more than 200 ARP requests are transmitted within 10s); the MAC address of a host maps to multiple IP addresses; the MAC address attempted to be updated based on an ARP request is different from the existing MAC address.

Configuration Example

Configuring Attack Detection

Configuration Steps	● Enable the local anti-attack function globally. ● Set the traffic attack threshold. ● Configure ARP attack detection.
	FS# configure terminal FS(config)# control-plane FS(config-cp)# ef-rnfp enable FS(config-cp)# attack threshold 500 FS(config-cp)# anti-arp-spoof scan 10 FS(config-cp)# anti-arp-spoof
Verification	● Display traffic attack information. ● Display ARP attack information.
	FS# show ip pim sparse-mode mroute FS# show attack-info current System currently not in attack! FS# show attack-info history System attack record at 1970-1-2 15:53:18, System in attack 8s ALL: 6958 packets, 584680 bytes PROTOCOL packets bytes ARP 1733 103980 UDP 5225 480700 TOP5 IP attack: IP packets bytes interface 172.18.3.84 2797 257324 Gi0/5 172.18.3.52 2428 223376 Gi0/5

```
172.18.3.80        1635        98100        Gi0/5
192.168.205.196    92          5520         Gi0/5
3.3.3.6            6           360          Gi0/5
FS#show arp-suspect
IP address         MAC address
192.168.1.1        00d0.f800.0002
```

3.4.3 Configuring the Local Anti-attack Whitelist

Configuration Effect

- When the device is attacked, whitelisted users can manage the device in Telnet or Web mode.

Notes

- Only add the IP address of the administrator to the whitelist.

Configuration Steps

Entering Global control-plane Mode

- Mandatory.

Configuring Whitelisted Users

- Optional.

Verification

Simulate network attacks to initiate device attacks, enable the local anti-attack, and configure whitelisted users.

- Non-whitelisted users feel stuck when telnetting to or accessing the Web page of the device, or fail to access the Web page of the device.
- Whitelisted users can telnet to and access the Web page of the device smoothly.

Related Commands

Configuring Anti-attack Whitelisted Users

Command	**security web permit** *low-ip-address* [*high-ip-address*]
Parameter Description	*low-ip-address*: Indicates the allowable IP address or the start IP address of the allowable IP address range. *group-or-source-address*: Indicates the end IP address of the allowable IP address range.
Command Mode	control-plane mode
Usage Guide	If a user configures security deny to deny Web access but needs to allow some specified IP addresses to access the Web page of the device, the user can run this command to add allowable IP addresses to the web permit IP whitelist. This command specifies the IP

	addresses that are allowed to access the Web page of the device (regardless of the local anti-attack rate limit and deny command).

Configuration Example

Configuring the Local Anti-attack Whitelist (Whitelisted IP Address Range: 192.168.1.2—192.168.1.10)

Configuration Steps	● Configure whitelisted users.
	FS# configure terminal FS(config)# control-plane FS(config-cp)# security web permit 192.168.1.2 192.168.1.10
Verification	Simulate network attacks and configure local anti-attack whitelisted users. ● Users not included in the local anti-attack whitelist cannot smoothly telnet to the device or access the Web page of the device. ● Users included in the local anti-attack whitelist can smoothly telnet to the device and access the Web page of the device.
	N/A

Common Errors

- All intranet users are added to the whitelist. As a result, the CPU utilization will be abnormal in the case of attacks from intranet users.

3.4.4 Configuring User Management Device Restriction

Configuration Effect

- After the ping operation is forbidden, non-whitelisted users cannot ping the device.
- After the Web access is forbidden, non-whitelisted users cannot access the Web page of the device.
- After Telnet and SSH login are forbidden, non-whitelisted users cannot telnet to the device or log in to the device in SSH mode.
- After SNMP management is forbidden, non-whitelisted users cannot manage the device over SNMP.

Notes

- This function can be used with the local anti-attack whitelist.

Configuration Steps

Entering Global control-plane Mode

- Mandatory.

Forbidding Intranet/Extranet Users to Ping the Device

- Optional.

Forbidding Intranet/Extranet Users to Access the Web Page of the Device

- Optional.

Forbidding Intranet/Extranet Users to Telnet to the Device or Log In to the Device in SSH Mode

- Optional.

Forbidding Intranet/Extranet Users to Manage the Device over SNMP

- Optional.

Verification

Enable the function of forbidding intranet/extranet users to ping the device, access the Web page of the device, telnet to the device or log in to the device in SSH mode, and manage the device over SNMP.

- Non-whitelisted users fail to ping the device, access the Web page of the device, telnet to the device or log in to the device in SSH mode, and mange the device over SNMP.
- Whitelisted users can ping the device, access the Web page of the device, telnet to the device or log in to the device in SSH mode, and mange the device SNMP.

Related Commands

Configuring User Management Device Restriction

Command	security deny { lan-ping | lan-web | wan-ping | wan-web | lan-telnet-ssh | lan-snmp | wan-telnet-ssh | wan-snmp }
Parameter Description	lan-ping: Forbids users to ping the device from a LAN port. lan-web: Forbids users to access the Web page of the device from a LAN port. wan-ping: Forbids users to ping the device from a WAN port. wan-web: Forbids users to access the Web page of the device from a WAN port. lan-telnet-ssh: Forbids users to telnet to the device or log in to the device in SSH mode from a LAN port. lan-snmp: Forbids users to manage the device over SNMP from a LAN port. wan-telnet-ssh: Forbids users to telnet to the device or log in to the device in SSH mode from a WAN port. wan-snmp: Forbids users to manage the device over SNMP from a WAN port.
Command Mode	control-plane mode
Usage Guide	If the functions are enabled but no whitelist is configured, you need to edit configurations through the console or Telnet.

Configuration Example

Configuring the Local Anti-attack Whitelist (Whitelisted IP Address Range: 192.168.1.2—192.168.1.10)

Configuration Steps	● Configure whitelisted users. ● Configure the functions of forbidding Intranet/Extranet users to ping the device, access the Web page of the device, telnet to the device or log in to the device in SSH mode, and manage the device over SNMP.
	FS# configure terminal FS(config)# control-plane FS(config-cp)# security web permit 192.168.1.2 192.168.1.10 FS(config-cp)# security deny wan-ping FS(config-cp)# security deny wan-web FS(config-cp)# security deny lan-ping FS(config-cp)# security deny lan-web FS(config-cp)# security deny lan-snmp FS(config-cp)# security deny wan-snmp FS(config-cp)# security deny lan-telnet-ssh FS(config-cp)# security deny wan-telnet-ssh FS(config-cp)#
Verification	● Non-whitelisted users cannot ping the device, access the Web page of the device, telnet to the device or log in to the device in SSH mode, and or mange the device over SNMP. ● Whitelisted users can ping the device, access the Web page of the device, telnet to the device or log in to the device in SSH mode, and mange the device over SNMP.

Common Errors

- After the ping operation and Web access are forbidden, but no user is added to the whitelist, users cannot log in to the Web page of the device.

3.5 Monitoring

Clearing

Description	Command
Clears historical attack information.	**clear attack-info history**

Displaying

Description	Command
Displays device anti-attack configurations and statistics.	**show ef-rnfp** {**acpp** { **data** | **manage** | **protocol** } | **scpp** { **data** | **manage** | **protocol** } | **glean-car** | **arp-car** | **port-filter** | **mpp** | **all** | **web-permit-ip** | **anti-arp-spoof** }

Displays current attack traffic.	**show attack-info current**
Displays historical attack traffic.	**show attack-info history**
Displays the ARP spoofing suspect list.	**show arp-suspect**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs local anti-attack.	**debug** { **acpp** | **scpp** | **glean-car** | **arp-car** | **port-filter** | **mpp** | **all** }
Records debugging data into the buffer.	**show ef-rnfp debug-buf clear**
Outputs debugging data.	**show ef-rnfp debug-buf echo**

4 Configuring SSH

4.1 Overview

Secure Shell (SSH) connection is similar to a Telnet connection except that all data transmitted over SSH is encrypted. When a user in an insecure network environment logs into a device remotely, SSH helps ensure information security and powerful authentication, protecting the device against attacks such as IP address spoofing and plain-text password interception.

An SSH-capable device can be connected to multiple SSH clients. In addition, the device can also function as an SSH client, and allows users to set up an SSH connection with a SSH-server device. In this way, the local device can safely log in to a remote device through SSH to implement management.

Currently, a device can work as either the SSH server or an SSH client, supporting SSHv1 and SSHv2 versions. FS SSH service supports both IPv4 and IPv6.

Unless otherwise specified, SSH in this document refers to SSHv2.

Protocols and Standards

- RFC 4251: The Secure Shell (SSH) Protocol Architecture
- RFC 4252: The Secure Shell (SSH) Authentication Protocol
- RFC 4253: The Secure Shell (SSH) Transport Layer Protocol
- RFC 4254: The Secure Shell (SSH) Connection Protocol
- RFC 4419: Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol
- RFC 4716: The Secure Shell (SSH) Public Key File Format
- RFC 4819: Secure Shell Public Key Subsystem
- RFC 3526: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 2409: The Internet Key Exchange (IKE)
- RFC 1950: ZLIB Compressed Data Format Specification version 3.3
- draft-ietf-secsh-filexfer-05: SSH File Transfer Protocol
- draft-ylonen-ssh-protocol-00: The version of the SSH Remote Login Protocol is 1.5. Comware implements the SSH server functions, but not the SSH client functions.

4.2 Applications

Application	Description
SSH Device Management	Use SSH to manage devices.
SSH Local Line Authentication	Use the local line password authentication for SSH user authentication.
SSH AAA Authentication	Use the authentication, authorization and accounting (AAA) mode for SSH user authentication.
SSH Public Key Authentication	Use the public key authentication for SSH user authentication.
SSH File Transfer	Use the Secure Copy (SCP) commands on the client to exchange

Application	Description
	data with the SSH server.

4.2.1 SSH Device Management

Scenario

You can use SSH to manage devices on the precondition that the SSH server function is enabled. By default, this function is disabled. The Telnet component that comes with the Windows system does not support SSH. Therefore, a third-party client software must be used. Currently, well-compatible software includes PuTTY, Linux, and SecureCRT. The following takes the PuTTY as an example to introduce the configurations of the SSH client. Figure 4-4-1 shows the network topology.

Figure 4-4-1 Networking Topology of SSH Device Management

Deployment

Configure the SSH client as follows:

- Start the PuTTY software.
- On the **Session** option tab of PuTTY, type in the host IP address of the SSH server and SSH port number **22**, and select the connection type **SSH**.
- On the **SSH** option tab of PuTTY, select the preferred SSH protocol version **2**.
- On the **SSH authentication** option tab of PuTTY, select the authentication method **Attempt "keyboard-interactive" auth**.
- Click **Open** to connect to the SSH server.
- Type in the correct user name and password to enter the terminal login interface.

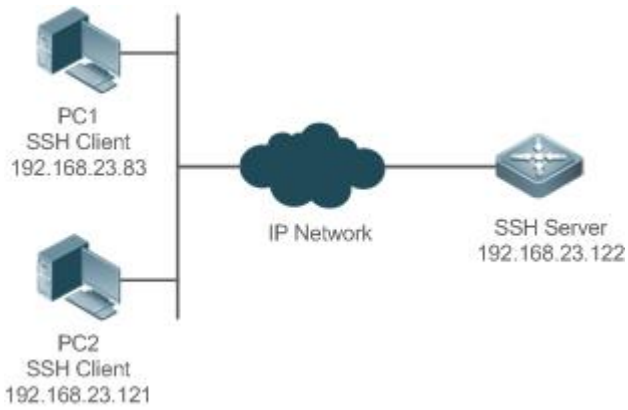
4.2.2 SSH Local Line Authentication

Scenario

SSH clients can use the local line password authentication mode, as shown in Figure 4-4-2.To ensure security of data exchange, PC 1 and PC 2 function as the SSH clients, and use the SSH protocol to log in to the network device where the SSH server function is enabled. The requirements are as follows:

- SSH users use the local line password authentication mode.
- Five lines, including Line 0 to Line 4, are activated concurrently. The login password is "passzero" for Line 0 and "pass" for the remaining lines. Any user name can be used.

Figure 4-4-2 Networking Topology of SSH Local Line Password Authentication



Deployment

- Configure the SSH server as follows:

1. Enable the SSH server function globally. By default, the SSH server supports two SSH versions: SSHv1 and SSHv2.
2. Configure the key. With this key, the SSH server decrypts the encrypted password received from the SSH clients, compares the decrypted plain text with the password stored on the server, and returns a message indicating the successful or unsuccessful authentication. SSHv1 uses an RSA key, whereas SSHv2 adopts an RSA or DSA key.
3. Configure the IP address of the FastEthernet 0/1 interface on the SSH server. The SSH client is connected to the SSH server using this IP address. The routes from the SSH clients to the SSH server are reachable.

- Configure the SSH client as follows:

Diversified SSH client software is available, including PuTTY,Linux, and OpenSSH. This document takes PuTTY as an example to explain the method for configuring the SSH clients.

14. Open the PuTTY connection tab, and select SSHv1 for authenticated login. (The method is similar if SSHv2 is selected.)
15. Set the IP address and connected port ID of the SSH server. As shown in the network topology, the IP address of the server is 192.168.23.122, and the port ID is 22. Click **Open** to start the connection. As the current authentication mode does not require a user name, you can type in any user name, but cannot be null. (In this example, the user name is "anyname".)

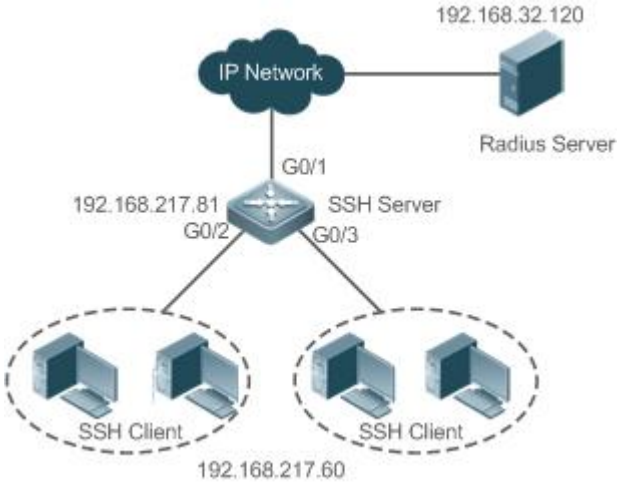
4.2.3 SSH AAA Authentication

Scenario

SSH users can use the AAA authentication mode for user authentication, as shown in Figure 4-4-3.To ensure security of data exchange, the PCs function as the SSH clients, and uses the SSH protocol to log in to the network device where the SSH server is enabled. To better perform security management, the AAA authentication mode is used for user login on the SSH clients. Two authentication methods, including Radius server authentication and local authentication, are provided in the AAA authentication method list to

ensure reliability. The Radius server authentication method is preferred. If the Radius server does not respond, it turns to the local authentication.

Figure 4-4-3 Networking Topology of SSH AAA Authentication



Deployment

- The routes from the SSH clients to the SSH server are reachable, and the route from the SSH server to the Radius server is also reachable.
- Configure the SSH server on the network device that functions as an SSH client.
- Configure the AAA parameters on the network device. When the AAA authentication mode is used, method lists are created to define the identity authentication and types, and applied to a specified service or interface.

4.2.4 SSH Public Key Authentication

Scenario

SSH clients can use the public keys for authentication, and the public key algorithm can be RSA or DSA, as shown in Figure 4-4-4.SSH is configured on the client so that a secure connection is set up between the SSH client and the SSH server.

Figure 4-4-4 Network Topology for Public Key Authentication of SSH Users

Deployment

- To implement public key authentication for the client, generate a key pair (RSA or DSA) on the client, configure the public key on the SSH server, and select the public key authentication mode.
- After the key is generated on the client, the SSH server will copy the file of the public key from the client to the flash and associates the file with the SSH user name. Each user can be associated with one RSA public key and one DSA public key.

4.2.5 SSH File Transfer

Scenario

The SCP service is enabled on the server, and SCP commands are used on the client to transfer data to the server, as shown in Figure 4-4-5.

Figure 4-4-5 Networking Topology of SSH File Transfer

Deployment

- Enable the SCP service on the server.
- On the client, use SCP commands to upload files to the server, or download files from the server.

4.3 Features

Basic Concepts

User Authentication Mechanism

- Password authentication

During the password authentication, a client sends a user authentication request and encrypted user name and password to the server. The server decrypts the received information, compares the decrypted information with those stored on the server, and then returns a message indicating the successful or unsuccessful authentication.

- Public key authentication

During the public key authentication, digital signature algorithms, such as RSA and DSA, are used to authenticate a client. The client sends a public key authentication request to the server. This request contains information including the user name, public key, and public key algorithm. On receiving the request, the server checks whether the public key is correct. If wrong, the server directly sends an authentication failure message. If right, the server performs digital signature authentication on the client, and returns a message indicating the successful or unsuccessful authentication.

Public key authentication is applicable only to the SSHv2 clients.

SSH Communication

To ensure secure communication, interaction between an SSH server and an SSH client undergoes the following seven stages:

- Connection setup

The server listens on Port 22 to the connection request from the client. After originating a socket initial connection request, the client sets up a TCP socket connection with the server.

- Version negotiation

If the connection is set up successfully, the server sends a version negotiation packet to the client. On receiving the packet, the client analyzes the packet and returns a selected protocol version to the server. The server analyzes the received information to determine whether version negotiation is successful.

- Key exchange and algorithm negotiation

If version negotiation is successful, key exchange and the algorithm negotiation are performed. The server and the client exchange the algorithm negotiation packet with each other, and determine the final algorithm based on their capacity. In addition, the server and the client work together to generate a session key and a session ID according to the key exchange algorithm and host key, which will be applied to subsequent user authentication, data encryption, and data decryption.

- User authentication

After the encrypted channel is set up, the client sends an authentication request to the server. The server repeatedly conducts authentication for the client until the authentication succeeds or the server shuts down the connection because the maximum number of authentication attempts is reached.

- Session request

After the successful authentication, the client sends a session request to the server. The server waits and processes the client request. After the session request is successfully processed, SSH enters the session interaction stage.

- Session interaction

After the session request is successfully processed, SSH enters the session interaction stage. Encrypted data can be transmitted and processed in both directions. The client sends a command to be executed to the client. The server decrypts, analyzes, and processes the received command, and then sends the encrypted execution result to the client. The client decrypts the execution result.

- Session ending

When the interaction between the server and the client is terminated, the socket connection disconnects, and the session ends.

Overview

Feature	Description
SSH Server	Enable the SSH server function on a network device, and you can set up a secure connection with the network device through the SSH client.
SCP Service	After the SCP service is enabled, you can directly download files from the network device and upload local files to the network device. In addition, all interactive data is encrypted, featuring authentication and security.

4.3.1 SSH Server

Enable the SSH server function on a network device, and you can set up a secure connection with the network device through the SSH client. You can also shut down the SSH server function to disconnect from all SSH clients.

Working Principle

For details about the working principle of the SSH server, see the "SSH Communication" in "Basic Concepts." In practice, after enabling the SSH server function, you can configure the following parameters according to the application requirements:

- Version: Configure the SSH version as SSHv1 orSSHv2 to connect SSH clients.
- Authentication timeout: The SSH server starts the timer after receiving a user connection request. The SSH server is disconnected from the client either when the authentication succeeds or when the authentication timeout is reached.
- Maximum number of authentication retries: The SSH server starts authenticating the client after receiving its connection request. If authentication does not succeed when the maximum number of user authentication retries is reached, a message is sent, indicating the authentication failure.
- Public key authentication: The public key algorithm can be RSA or DSA. It provides a secure connection between the client and the server. The public key file on the client is associated with the user name. In addition, the public key authentication mode is configured on the client, and the corresponding private key file is specified. In this way, when the client attempts to log in to the server, public key authentication can be implemented to set up a secure connection.

Related Configuration

Enabling the SSH Server

By default, the SSH server is disabled.

In global configuration mode, run the [**no**] **enable service ssh-server** command to enable or disable the SSH server.

To generate the SSH key, you also need to enable the SSH server.

Specifying the SSH Version

By default, the SSH server supports both SSHv1 and SSHv2, connecting either SSHv1 clients or SSHv2 clients.

Run the **ip ssh version** command to configure the SSH version supported by the SSH server.

If only SSHv1 or SSHv2 is configured, only the SSH client of the configured version can be connected to the SSH server.

Configuring the SSH Authentication Timeout

By default, the user authentication timeout is 120s.

Run the **ip ssh time-out** command to configure the user authentication timeout of the SSH server. Use the **no** form of the command to restore the default timeout. The SSH server starts the timer after receiving a user connection request. If authentication does not succeed before the timeout is reached, authentication times out and fails.

Configuring the Maximum Number of SSH Authentication Retries

By default, the maximum number of user authentication retries is 3.

Run the **ip ssh authentication-retries** command to configure the maximum number of user authentication retries on the SSH server. Use the **no** form of the command to restore the default number of user

authentication retries. If authentication still does not succeed when the maximum number of user authentication retries is reached, user authentication fails.

Specifying the SSH Encryption Mode

By default, the encryption mode supported by the SSH server is Compatible, that is, supporting cipher block chaining (CBC), counter (CTR) and other encryption modes.

Run the **ip ssh cipher-mode** command to configure the encryption mode supported by the SSH server. Use the **no** form of the command to restore the default encryption mode supported by the SSH server.

Specifying the SSH Message Authentication Algorithm

By default, the message authentication algorithms supported by the SSH server are as follows: (1) For the SSHv1, no algorithm is supported; (2) For the SSHv2, four algorithms, including MD5,SHA1,SHA1-96, and MD5-96, are supported.

Run the **ip ssh hmac-algorithm** command to configure the message authentication algorithm supported by the SSH server. Use the **no** form of the command to restore the default message authentication algorithm supported by the SSH server.

Enabling the Public Key Authentication on the SSH Server

Run the **ip ssh peer** command to associate the public key file on the client with the user name. When the client is authenticated upon login, a public key file is specified based on the user name.

4.3.2 SCP Service

The SSH server provides the SCP service to implement secure file transfer between the server and the client.

Working Principle

- SCP is a protocol that supports online file transfer. It runs on Port 22 based on the BSC RCP protocol, whereas RCP provides the encryption and authentication functions based on the SSH protocol. RCP implements file transfer, and SSH implements authentication and encryption.
- Assume that the SCP service is enabled on the server. When you use an SCP client to upload or download files, the SCP client first analyzes the command parameters, sets up a connection with a remote server, and starts another SCP process based on this connection. This process may run in source or sink mode. (The process running in source mode is the data provider. The process running in sink mode is the destination of data.) The process running in source mode reads and sends files to the peer end through the SSH connection. The process running in sink mode receives files through the SSH connection.

Related Configuration

Enabling the SCP Server

By default, the SCP server function is disabled.

Run the **ip scp server enable** command to enable SCP server function on a network device.

4.4 Configuration

Configuration	Description and Command	
Configuring the SSH Server	It is mandatory to enable the SSH server.	
	enable service ssh-server	Enables the SSH server.
	disconnect ssh[**vty**] *session-id*	Disconnects an established SSH session.
	crypto key generate {**rsa**|**dsa**}	Generates an SSH key.
	ip ssh version {**1**|**2**}	Specifies the SSH version.
	ip ssh time-out *time*	Configures the SSH authentication timeout.
	ip ssh authentication-retries *retry times*	Configures the maximum number of SSH authentication retries.
	Ip ssh cipher-mode{**cbc** | **ctr** | **others** }	Specifies the SSH encryption mode.
	Ip ssh hmac-algorithm{**md5** | **md5-96** | **sha1** | **sha1-96**}	Specifies the SSH message authentication algorithm.

4.4.1 Configuring the SSH Server

Configuration Effect

- Enable the SSH server function on a network device so that you can set up a secure connection with a remote network device through the SSH client. All interactive data is encrypted before transmitted, featuring authentication and security.
- You can use diversified SSH user authentications modes, including local line password authentication, AAA authentication, and public key authentication.
- You can generate or delete an SSH key.
- You can specify the SSH version.
- You can configure the SSH authentication timeout.
- You can configure the maximum number of SSH authentication retries.
- You can specify the SSH encryption mode.
- You can specify the SSH message authentication algorithm.
- You can specify ACL filtering of the SSH server.

Notes

- The precondition of configuring a device as the SSH server is that communication is smooth on the network that the device resides, and the administrator can access the device management interface to configure related parameters.
- The **no crypto key generate** command does not exist. You need to run the **crypto key zeroize** command to delete a key.

- The SSH module does not support hot standby. Therefore, for products that supports hot standby on the supervisor modules, if no SSH key file exist on the new active module after failover, you must run the **crypto key generate** command to re-generate a key before using SSH.

Configuration Steps

Enabling the SSH Server

- Mandatory.
- By default, the SSH server is disabled. In global configuration mode, enable the SSH server and generate an SSH key so that the SSH server state changes to ENABLE.

Specifying the SSH Version

- Optional.
- By default, the SSH server supports SSHv1 and SSHv2, connecting either SSHv1 or SSHv2clients. If only SSHv1 or SSHv2 is configured, only the SSH client of the configured version can be connected to the SSH server.

Configuring the SSH Authentication Timeout

- Optional.
- By default, the SSH authentication timeout is 120s. You can configure the user authentication timeout as required. The value ranges from 1 to 120. The unit is second.

Configuring the Maximum Number of SSH Authentication Retries

- Optional.
- Configure the maximum number of SSH authentication retries to prevent illegal behaviors such as malicious guessing. By default, the maximum number of SSH authentication retries is 3, that is, a user is allowed to enter the user name and password three times for authentication. You can configure the maximum number of retries as required. The value ranges from 0 to 5.

Specifying the SSH Encryption Mode

- Optional.
- Specify the encryption mode supported by the SSH server. By default, the encryption mode supported by the SSH server is Compatible, that is, supporting CBC, CTR and other encryption modes.

Specifying the SSH Message Authentication Algorithm

- Optional.
- Specify the message authentication algorithm supported by the SSH server. By default, the message authentication algorithms supported by the SSH server are as follows: (1) For the SSHv1, no algorithm is supported; (2) For the SSHv2, four algorithms, including MD5, SHA1, SHA1-96, and MD5-96, are supported.

Setting ACL Filtering of the SSH Server

- Optional.

- Set ACL filtering of the SSH server. By default, ACL filtering is not performed for all connections to the SSH server. According to needs, set ACL filtering to perform for all connections to the SSH server.

Enabling the Public Key Authentication for SSH Users

- Optional.
- Only SSHv2 supports authentication based on the public key. This configuration associates a public key file on the client with a user name. When a client is authenticated upon login, a public key file is specified based on the user name.

Verification

- Run the **show ip ssh** command to display the current SSH version, authentication timeout, and maximum number of authentication retries of the SSH server.
- Run the **show crypto key mypubkey** command to display the public information of the public key to verify whether the key has been generated.
- Configure the public key authentication login mode on the SSH client and specify the private key file. Check whether you can successfully log in to the SSH server from the SSH client. If yes, the public key file on the client is successfully associated with the user name, and public key authentication succeeds.

Related Commands

Enabling the SSH Server

Command	**enable service ssh-server**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	To disable the SSH server, run the **no enable service ssh-server** command in global configuration mode. After this command is executed, the SSH server state changes to DISABLE.

Disconnecting an Established SSH Session

Command	**disconnect ssh**[**vty**] *session-id*
Parameter Description	**vty:** Indicates an established virtual teletype terminal (VTY) session. *session-id*: Indicates the ID of the established SSH session. The value ranges from 0 to 35.
Command Mode	Privileged EXEC mode
Usage Guide	Specify an SSH session ID to disconnect the established SSH session. Alternatively, specify a VTY session ID to disconnect a specified SSH session. Only an SSH session can be disconnected.

Generating an SSH Key

Command	**crypto key generate** {**rsa**|**dsa**}
Parameter	**rsa:** Generates an RSA key.

Description	**dsa:** Generates a DSA key.
Command Mode	Global configuration mode
Usage Guide	The **no crypto key generate** command does not exist. You need to run the **crypto key zeroize** command to delete a key. SSHv1 uses an RSA key, whereas SSHv2 uses an RSA or DSA key. If an RSA key is generated, both SSHv1 and SSHv2 are supported. If only a DSA key is generated, only SSHv2 can use the key.

Specifying the SSH Version

Command	**ip ssh version** {**1**|**2**}
Parameter Description	**1:** Indicates that the SSH server only receives the connection requests sent by SSHv1 clients. **2:** Indicates that the SSH server only receives the connection requests sent by SSHv2 clients.
Command Mode	Global configuration mode
Usage Guide	Run the **no ip ssh version** command to restore the default settings. By default, the SSH server supports both SSHv1 and SSHv2.

Configuring the SSH Authentication Timeout

Command	**ip ssh time-out** *time*
Parameter Description	*time*: Indicates the SSH authentication timeout. The value ranges from 1 to 120. The unit is second.
Command Mode	Global configuration mode
Usage Guide	Run the **no ip ssh time-out** command to restore the default SSH authentication timeout, which is 120s.

Configuring the Maximum Number of SSH Authentication Retries

Command	**ip ssh authentication-retries** *retry times*
Parameter Description	*retry times*: Indicates the maximum number of user authentication retries. The value ranges from 0 to 5.
Command Mode	Global configuration mode
Usage Guide	Run the **no ip ssh authentication-retries** command to restore the default number of user authentication retries, which is 3.

Specifying the SSH Encryption Mode

Command	**ip ssh cipher-mode**{**cbc** | **ctr** | **others** }
Parameter Description	**cbc:** Sets the encryption mode supported by the SSH server to the CBC mode. Corresponding algorithms include DES-CBC,3DES-CBC,AES-128-CBC,AES-192-CBC,AES-256-CBC, and Blowfish-CBC. **ctr:** Sets the encryption mode supported by the SSH server to the CTR mode. Corresponding algorithms include AES128-CTR, AES192-CTR, and AES256-CTR.

	others: Sets the encryption mode supported by the SSH server to others. The corresponding algorithm is RC4.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the encryption mode supported by the SSH server. On FS devices, the SSHv1 server supports the DES-CBC, 3DES-CBC, and Blowfish-CBC encryption algorithms; the SSHv2 server supports the AES128-CTR, AES192-CTR, AES256-CTR, DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, Blowfish-CBC, and RC4 encryption algorithms. These algorithms can be grouped into three encryption modes: CBC, CTR, and others. As the cryptography continuously develops, it is approved that encryption algorithms in the CBC and others modes can be decrypted in a limited period of time. Therefore, organizations or companies that have high security requirements can set the encryption mode supported by the SSH server to CTR to increase the security level of the SSH server.

Specifying the SSH Message Authentication Algorithm

Command	**ip ssh hmac-algorithm**{**md5** | **md5-96** | **sha1** | **sha1-96**}
Parameter Description	**md5:** Indicates that the message authentication algorithm supported by the SSH server is MD5. **md5-96:** Indicates that the message authentication algorithm supported by the SSH server is MD5-96. **sha1:** Indicates that the message authentication algorithm supported by the SSH server is SHA1. **sha1-96:** Indicates that the message authentication algorithm supported by the SSH server is SHA1-96.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the message authentication algorithm supported by the SSH server. On FS devices, the SSHv1 server does support any message authentication algorithm; the SSHv2 server supports the MD5, SHA1, SHA1-96, **and** MD5-96 message authentication algorithms. You can select message authentication algorithms supported by the SSH server as required.

Configuring RSA Public Key Authentication

Command	**ip ssh peer** *test* **public-key rsaflash**:*rsa.pub*
Parameter Description	*test*: Indicates the user name. **rsa:** Indicates that the public key type is RSA. *rsa.pub*: Indicates the name of a public key file.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the RSA public key file associated with user *test*. Only SSHv2 supports authentication based on the public key. This command associates the public key file on the client with the user name. When the client is authenticated upon login,

	a public key file is specified based on the user name.

Configuring DSA Public Key Authentication

Command	**ip ssh peer** *test* **public-key dsaflash**:*dsa.pub*
Parameter Description	*test*: Indicates the user name. **dsa**: Indicates that the public key type is DSA. *dsa.pub*: Indicates the name of a public key file.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the DSA key file associated with user **test**. Only SSHv2 supports authentication based on the public key. This command associates the public key file on the client with the user name. When the client is authenticated upon login, a public key file is specified based on the user name.

Configuration Example

The following configuration examples describe only configurations related to SSH.

Generating a Public Key on the SSH Server

Configuration Steps	● Run the **crypto key generate { rsa | dsa }** command to generate a RSA public key for the server.
SSH Server	FS#configure terminal FS(config)# crypto key generate rsa Choose the size of the rsa key modulus in the range of 512 to 2048 and the size of the dsa key modulus in the range of 360 to 2048 for your Signature Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: ● If the generation of the RSA key is successful, the following information is displayed: % Generating 512 bit RSA1 keys ...[ok] % Generating 512 bit RSA keys ...[ok] ● If the generation of the RSA key fails, the following information is displayed: % Generating 512 bit RSA1 keys ...[fail] % Generating 512 bit RSA keys ...[fail]
Verification	● Run the **show crypto key mypubkey rsa** command to display the public information about the RSA key. If the public information about the RSA key exists, the RSA key has been generated.

SSH Server	FS(config)#show crypto key mypubkey rsa % Key pair was generated at: 1:49:47 UTC Jan 4 2013 Key name: RSA1 private Usage: SSH Purpose Key Key is not exportable. Key Data: AAAAAwEA AQAAAHJM 6izXt1pp rUSOEGZ/ UhFpRRrW nngP4BU7 mG836apf jajSYwcU 8O3LojHL ayJ8G4pG 7j4T4ZSf FKg09kfr 92JpRNHQ gbwaPc5/ 9UnTtX9t qFIKDj1j 0dKBcCfN tr0r/CT+ cs5tlGKV S0ICGifz oB+pYaE= % Key pair was generated at: 1:49:47 UTC Jan 4 2013 Key name: RSA private Usage: SSH Purpose Key Key is not exportable. Key Data: AAAAAwEAAQAAAHJfLwKnzOgO F3RlKhTN /7PmQYoE v0a2VXTX 8ZCa7Sll EghLDLJc w3T5JQXk Rr3iBD5s b1EeOL4b 21ykZt/u UetQ0Q80 sISglfZ9 8o5No3Zz MPM0LnQR G4c7/28+ GOHzYkTk 4liQuTIL HRgtbyEYXCFaaxU=

Specifying the SSH Version

Configuration Steps	● Run the **ip ssh version** { **1** | **2** } command to set the version supported by the SSH server to SSHv2.
SSH Server	FS#configure terminal FS(config)#ip ssh version 2
Verification	● Run the **show ip ssh** command to display the SSH version currently supported by the SSH server.
SSH Server	FS(config)#show ip ssh SSH Enable - version 2.0 Authentication timeout: 120 secs Authentication retries: 3 SSH SCP Server: disabled

Configuring the SSH Authentication Timeout

Configuratio	● Run the **ip ssh time-out** *time* command to set the SSH authentication timeout to 100s.

n Steps	
SSH Server	FS#configure terminal FS(config)#ip sshtime-out100
Verification	● Run the **show ip ssh** command to display the configured SSH authentication timeout.
SSH Server	FS(config)#show ip ssh SSH Enable - version 2.0 Authentication timeout: 100 secs Authentication retries: 3 SSH SCP Server: disabled

Configuring the Maximum Number of SSH Authentication Retries

Configuration Steps	● Run the **ip ssh authentication-retries** *retry times* command to set the maximum number of user authentication retries on the SSH server to 2.
SSH Server	FS#configure terminal FS(config)#ip ssh authentication-retries 2
Verification	● Run the **show ip ssh** command to display the configured maximum number of authentication retries.
SSH Server	FS(config)#show ip ssh SSH Enable - version 2.0 Authentication timeout: 100 secs Authentication retries: 3 SSH SCP Server: disabled

Specifying the SSH Encryption Mode

Configuration Steps	● Run the **ip ssh cipher-mode** {**cbc** | **ctr** | **others** }command to set the encryption mode supported by the SSH server to CTR.
SSH Server	FS#configure terminal FS(config)# ip ssh cipher-mode ctr
Verification	● Select the CTR encryption mode on the SSH client, and verify whether you can successfully log in to the SSH server from the SSH client.

Specifying the SSH Message Authentication Algorithm

Configuration Steps	● Run the **ip ssh hmac-algorithm** {**md5** | **md5-96** | **sha1** | **sha1-96** } command to set the message authentication algorithm supported by the SSH server to SHA1.

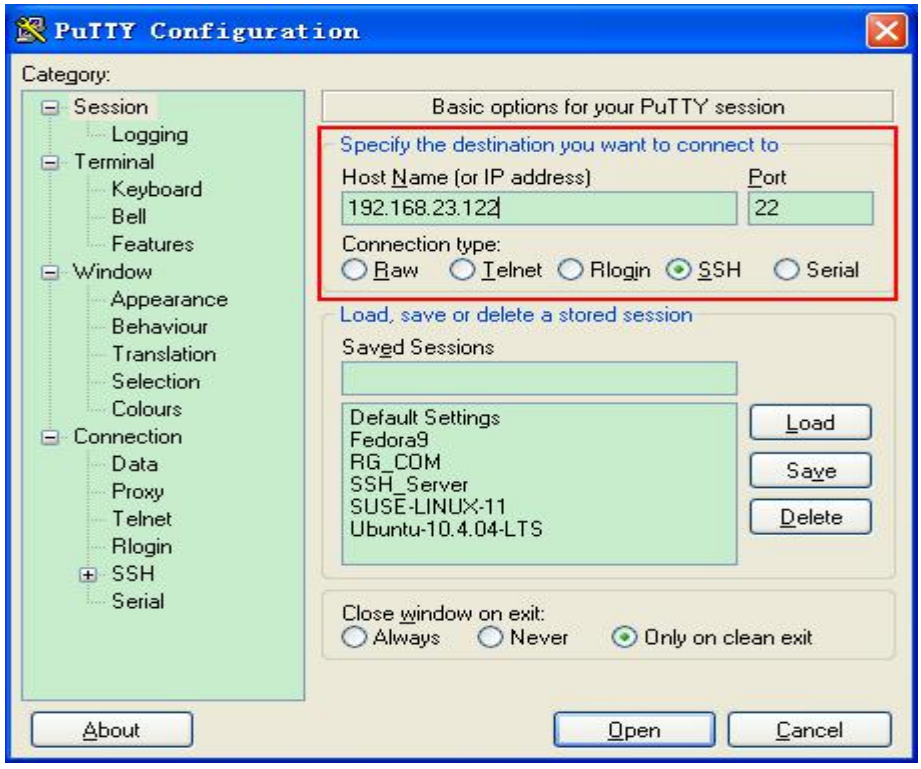
SSH Server	FS#configure terminal FS(config)# ip ssh hmac-algorithmsha1
Verification	● Select the SHA1 message authentication algorithm on the SSH client, and verify whether you can successfully log in to the SSH server from the SSH client.

Configuring the Public Key Authentication

Configuration Steps	● Run the **ip ssh peer** *username* **public-key** { **rsa** | **dsa**}*filename* command to associate a public key file of the client with a user name. When the client is authenticated upon login, a public key file (for example, RSA) is specified based on the user name.
SSH Server	FS#configure terminal FS(config)# ip ssh peer test public-key rsaflash:rsa.pub
Verification	● Configure the public key authentication login mode on the SSH client and specify the private key file. Check whether you can successfully log in to the SSH server from the SSH client. If yes, the public key file on the client is successfully associated with the user name, and public key authentication succeeds.

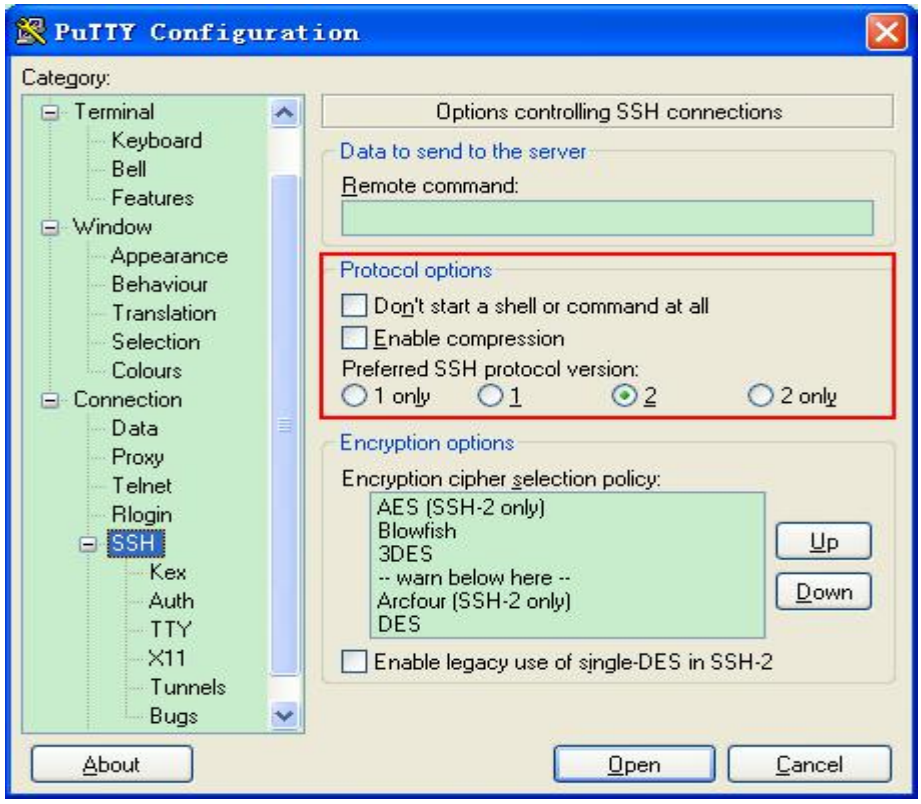
Configuring SSH Device Management

Scenario Figure 4-6	 You can use SSH to manage devices on the precondition that the SSH server function is enabled. By default, this function is disabled. The Telnet component that comes with the Windows does not support SSH. Therefore, a third-party client software must be used. Currently, well-compatible client software includes PuTTY, Linux, and SecureCRT. The following takes the PuTTY as an example to introduce the configurations of the SSH client.
Configuration Steps	● Start the PuTTY software. ● On the **Session** option tab of PuTTY, type in the host IP address **192.168.23.122** and SSH port number **22**, and select the connection type **SSH**. ● On the **SSH** option tab of PuTTY, select the preferred SSH protocol version **2**. ● On the **SSH authentication** option tab of PuTTY, select the authentication method **Attempt "keyboard-interactive" auth**. ● Click **Open** to connect to the SSH server. ● Type in the correct user name and password to enter the terminal login interface.
SSH Client	Figure 4-4-6



Host Name (or IP address) indicates the IP address of the host to be logged in. In this example, the IP address is **192.168.23.122**. **Port** indicates the port ID 22, that is, the default ID of the port listened by SSH. **Connection type** is **SSH**.

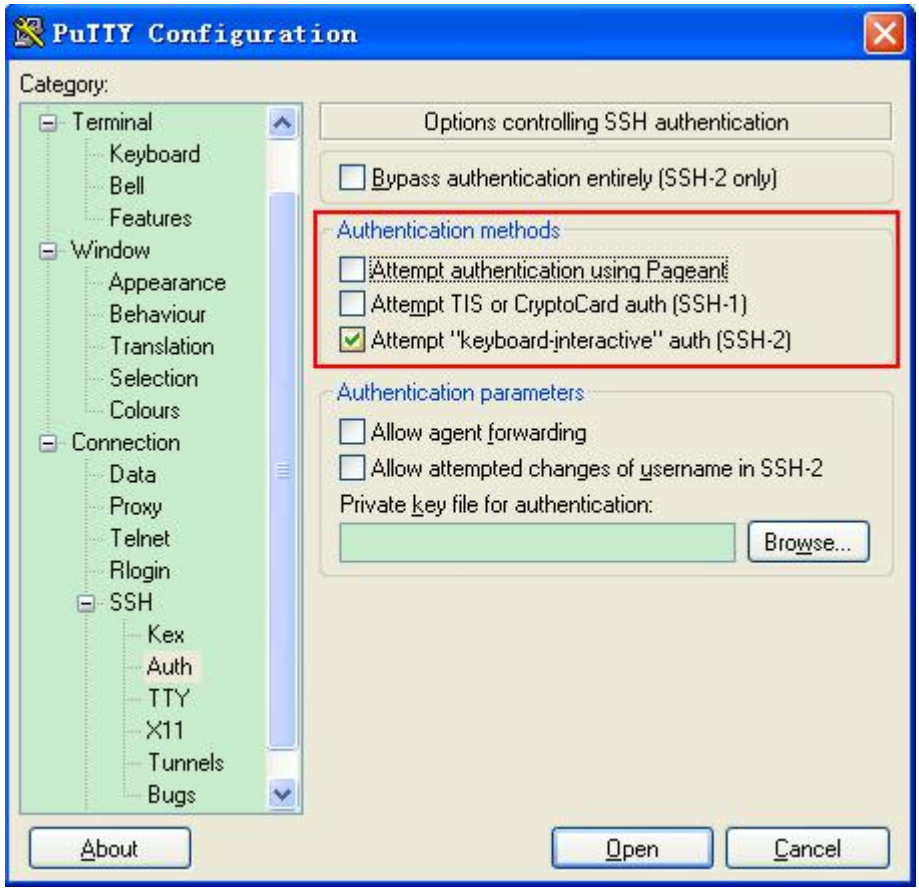
Figure 4-4-7



As shown in Figure 4-4-7, select **2** as the preferred SSH protocol version in the **Protocol**

options pane because SSHv2 is used for login.

Figure 4-4-8



As shown in Figure 4-8, select **Attempt "keyboard-interactive" auth** as the authentication method to support authentication based on the user name and password.

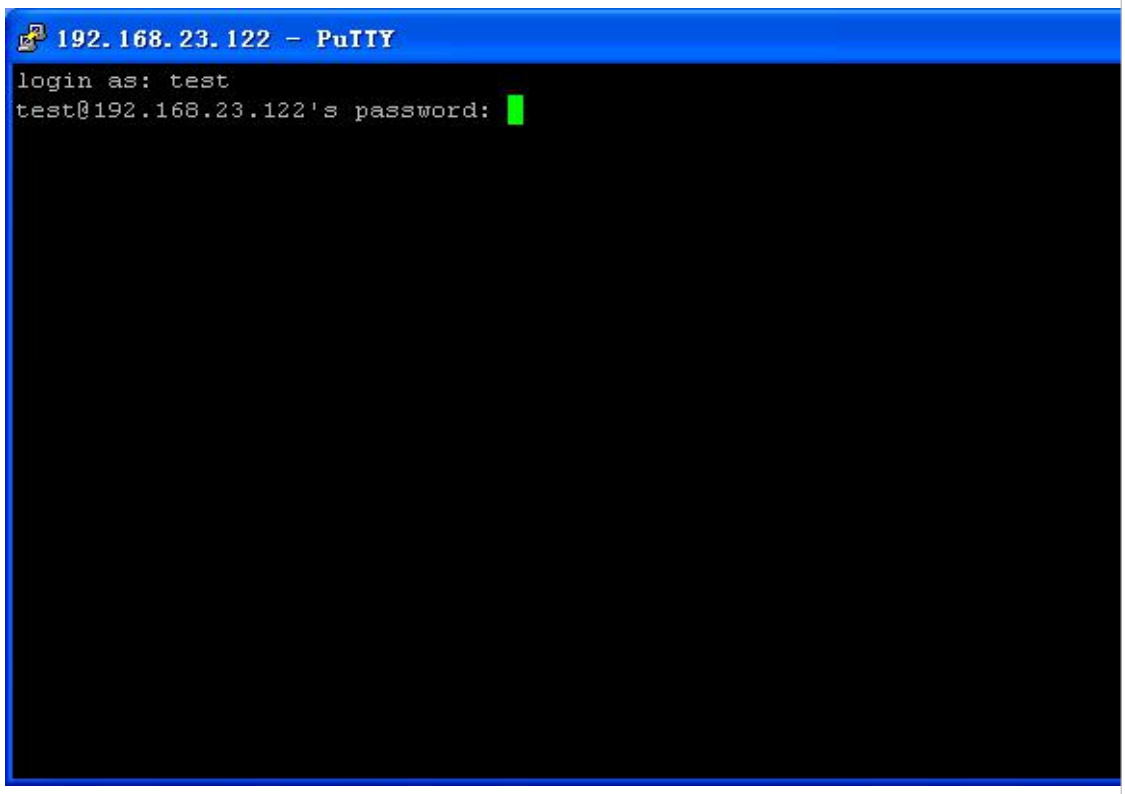
Then, click **Open** to connect to the configured server host, as shown in Figure 4-4-9.

Figure 4-4-9

The **PuTTY Security Alert** box indicates that you are logging in to the client of the server 192.168.23.122, and asks you whether to receive the key sent from the server.

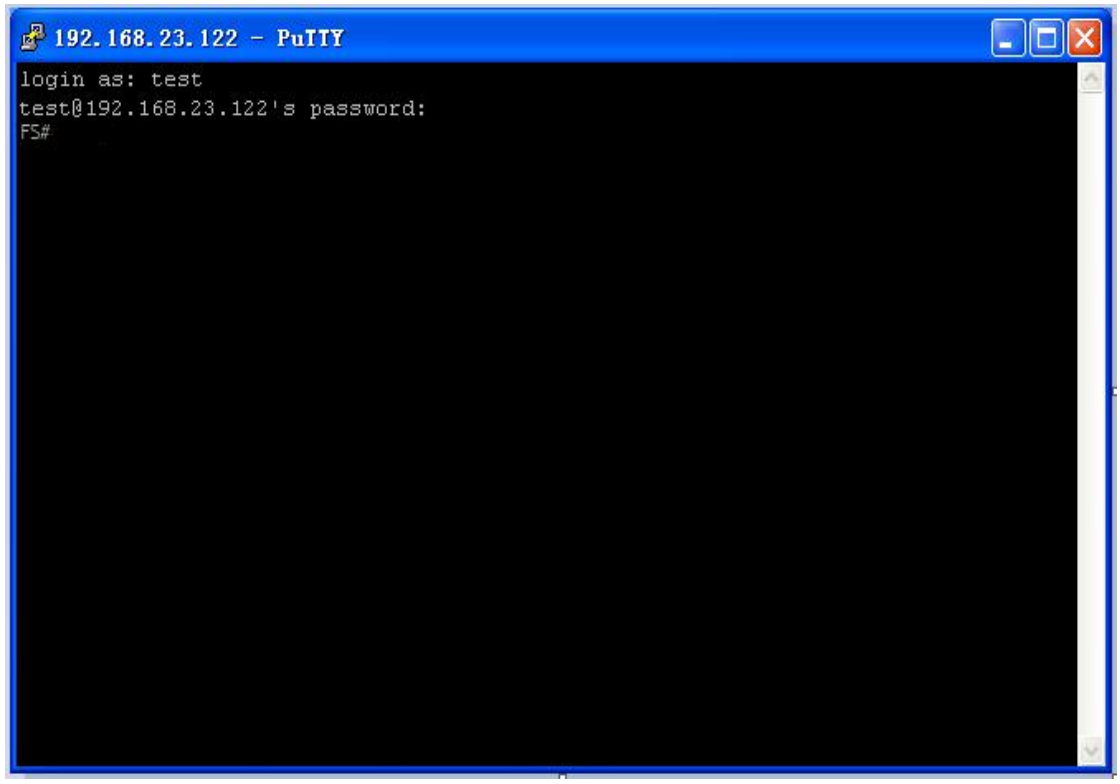
If you select **Yes**, a login dialog box is displayed, as shown in Figure4-4-10.

Figure4-4-10



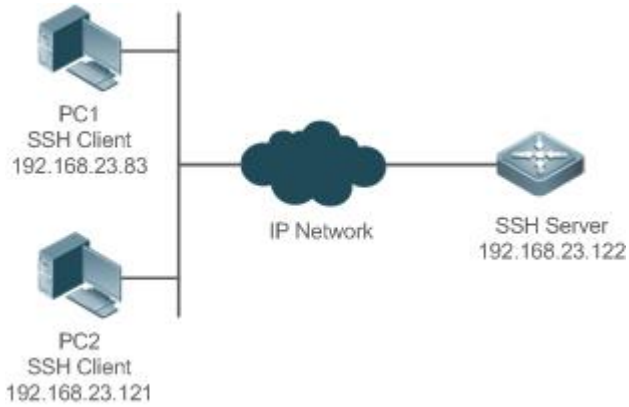
Type in the correct user name and password, and you can log in to the SSH terminal interface, as shown in Figure 4-4-11.

Figure 4-4-11

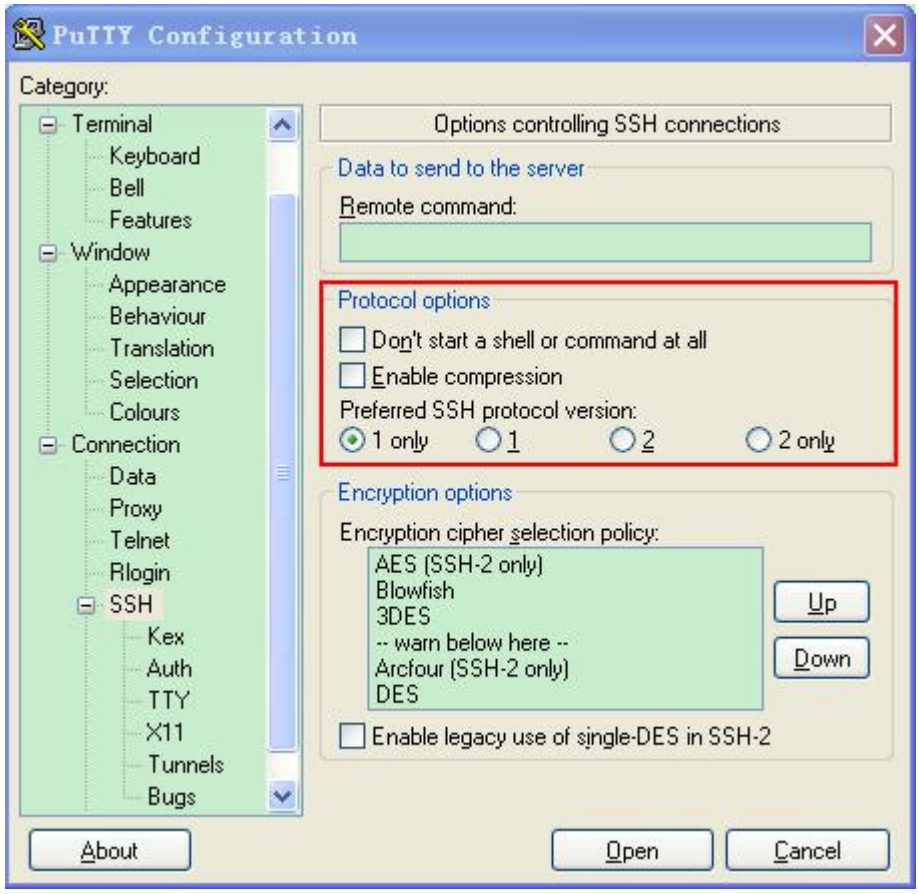


Verification	● Run the **show ip ssh** command to display the configurations that are currently effective on the SSH server. ● Run the **show ssh** command to display information about every SSH connection that has been established.
	FS#show ip ssh SSH Enable - version 1.99 Authentication timeout: 120 secs Authentication retries: 3 FS#show ssh Connection Version Encryption Hmac State Username 0 2.0 aes256-cbc hmac-sha1 Session started test

Configuring SSH Local Line Authentication

Scenario Figure 4-4-12	 SSH users can use the local line password for user authentication, as shown in Figure 4-4-12.To ensure security of data exchange, PC 1 and PC 2 function as the SSH clients, and use the SSH protocol to log in to the network device where the SSH server is enabled. The requirements are as follows: ● SSH users use the local line password authentication mode. ● Five lines, including Line 0 to Line 4, are activated concurrently. The login password is "passzero" for Line 0 and "pass" for the remaining lines. Any user name can be used.
Configuration Steps	Configure the SSH server as follows: ● Enable the SSH server function globally. By default, the SSH server supports two SSH versions: SSHv1 and SSHv2. ● Configure the key. With this key, the SSH server decrypts the encrypted password received from the SSH client, compares the decrypted plain text with the password stored on the server, and returns a message indicating the successful or unsuccessful authentication. SSHv1 uses the RSA key, whereas SSHv2 uses the RSA or DSA key. ● Configure the IP address of the FastEthernet 0/1 interface on the SSH server. The SSH client is connected to the SSH server based on this IP address. The route from the SSH

	client to the SSH server is reachable. Configure the SSH client as follows: ● Diversified SSH client software is available, including PuTTY, Linux, and SecureCRT. This document takes PuTTY as an example to explain the method for configuring the SSH client. For details about the configuration method, see "Configuration Steps."
SSH Server	Before configuring SSH-related function, ensure that the route from the SSH user to the network segment of the SSH server is reachable. The interface IP address configurations are shown in Figure 4-4-13. The detailed procedures for configuring IP addresses and routes are omitted. FS(config)# enable service ssh-server FS(config)#crypto key generate rsa % You already have RSA keys. % Do you really want to replace them? [yes/no]: Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: % Generating 512 bit RSA1 keys ...[ok] % Generating 512 bit RSA keys ...[ok] FS(config)#interface fastEthernet0/1 FS(config-if-fastEthernet0/1)#ip address 192.168.23.122 255.255.255.0 FS(config-if-fastEthernet0/1)#exit FS(config)#line vty 0 FS(config-line)#password passzero FS(config-line)#privilege level 15 FS(config-line)#login FS(config-line)#exit FS(config)#line vty1 4 FS(config-line)#password pass FS(config-line)#privilege level 15 FS(config-line)#login FS(config-line)#exit
SSH Client(PC1/PC2)	Figure 4-4-13



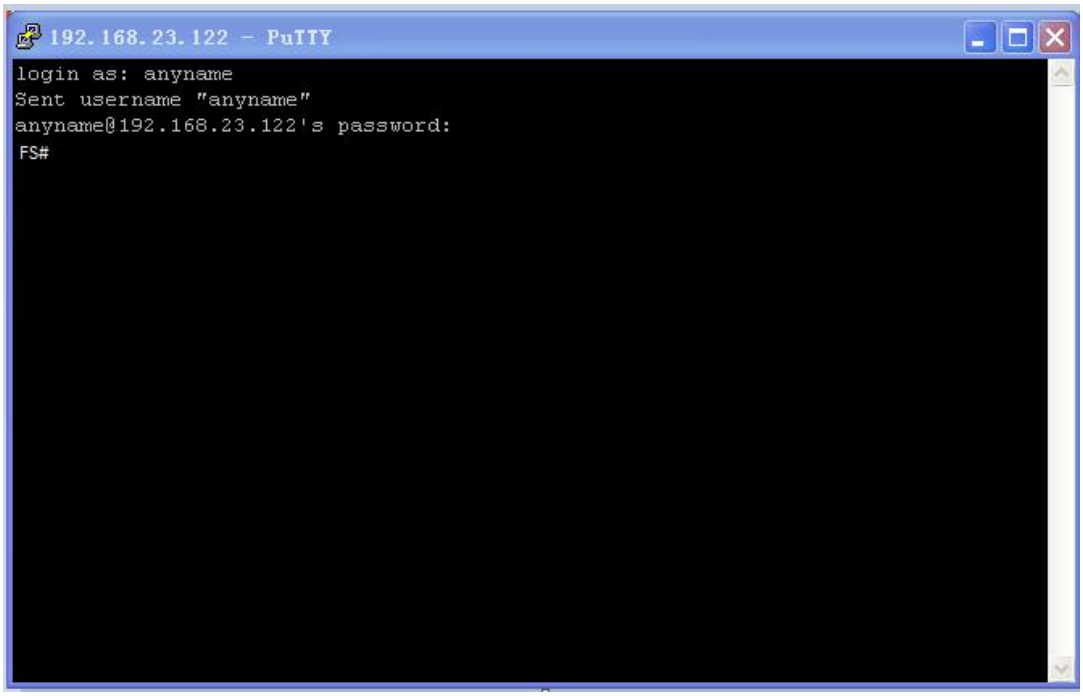
Set the IP address and port ID of the SSH server. As shown in the network topology, the IP address of the server is 192.168.23.122, and the port ID is 22 (For details about the configuration method, see "Configuring SSH Device Management."). Click **Open** to start the SSH server. As the current authentication mode does not require a user name, you can type in any user name, but cannot leave the user name unspecified. (In this example, the user name is "anyname".)

Verification

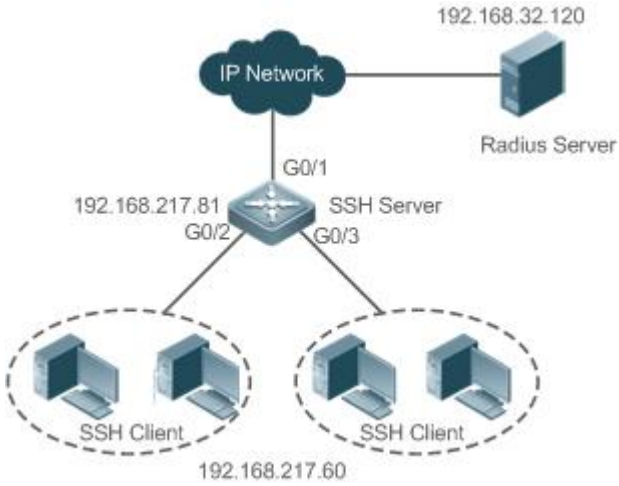
- Run the **show running-config** command to display the current configurations.
- Verify that the SSH client configurations are correct.

SSH Server

```
FS#show running-config

Building configuration...

!

enable secret 5 $1$eyy2$xs28FDw4s2q0tx97

enable service ssh-server

!

interface fastEthernet0/1

ip address 192.168.23.122 255.255.255.0

!

line vty 0
```

	privilege level 15 login password passzero line vty 1 4 privilege level 15 login password pass ! end
SSH Client	Set up a connection, and enter the correct password. The login password is "passzero" for Line 0 and "pass" for the remaining lines. Then, the SSH server operation interface is displayed, as shown in Figure 4-4-14. Figure 4-4-14  FS#show users Line User Host(s) Idle Location ---------- ---------- ---------- ---------- ---------- * 0 con 0 --- idle 00:00:00 --- 1 vty 0 --- idle 00:08:02 192.168.23.83 2 vty 1 --- idle 00:00:58 192.168.23.121

Configuring AAA Authentication of SSH Users

Scenario Figure 4-4-15	 SSH users can use the AAA authentication mode for user authentication, as shown in Figure 4-4-15.To ensure security of data exchange, the PC functions as the SSH client, and uses the SSH protocol to log in to the network device where the SSH server is enabled. To better perform security management, the AAA authentication mode is used on the user login interface of the SSH client. Two authentication methods, including Radius server authentication and local authentication, are provided in the AAA authentication method list to ensure reliability. The Radius server authentication method is preferred. If the Radius server does not respond, select the local authentication method.
Configuration Steps	● The route from the SSH client to the SSH server is reachable, and the route from the SSH server to the Radius server is also reachable. ● Configure the SSH server on the network device. The configuration method is already described in the previous example, and therefore omitted here. ● Configure the AAA parameters on the network device. When the AAA authentication mode is used, method lists are created to define the identity authentication and types, and applied to a specified service or interface.
SSH Server	FS(config)# enable service ssh-server FS(config)#crypto key generate rsa % You already have RSA keys. % Do you really want to replace them? [yes/no]: Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: % Generating 512 bit RSA1 keys ...[ok] % Generating 512 bit RSA keys ...[ok] FS(config)#crypto key generate dsa

```
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit DSA keys ...[ok]
FS(config)#interface gigabitEthernet1/1
FS(config-if-gigabitEthernet1/1)#ip address 192.168.217.81 255.255.255.0
FS(config-if-gigabitEthernet1/1)#exit
FS#configure terminal
FS(config)#aaa new-model
FS(config)#radius-server host 192.168.32.120
FS(config)#radius-server key aaaradius
FS(config)#aaa authentication login methodgroup radius local
FS(config)#line vty 0 4
FS(config-line)#login authentication method
FS(config-line)#exit
FS(config)#username user1 privilege 1 password 111
FS(config)#username user2 privilege 10 password 222
FS(config)#username user3 privilege 15 password 333
FS(config)#enable secret w
```

Verification

- Run the **show running-config** command to display the current configurations.
- This example assumes that the SAM server is used.
- Set up a remote SSH connection on the PC.
- Check the login user.

```
FS#show run
aaa new-model
!
aaa authentication login method group radius local
!
username user1 password 111
username user2 password 222
username user2 privilege 10
username user3 password 333
username user3 privilege 15
```

```
no service password-encryption
!
radius-server host 192.168.32.120
radius-server key aaaradius
enable secret 5 $1$hbgz$ArCsyqty6yyzzp03
enable service ssh-server
!
interface gigabitEthernet1/1
 no ip proxy-arp
ip address 192.168.217.81 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.217.1
!
line con 0
line vty 0 4
 login authentication method
!
End
```

On the SSH client, choose **System Management**>**Device Management**, and add the device IP address **192.168.217.81** and the device key **aaaradius**.

Choose **Security Management**>**Device Management Rights**, and set the rights of the login user.

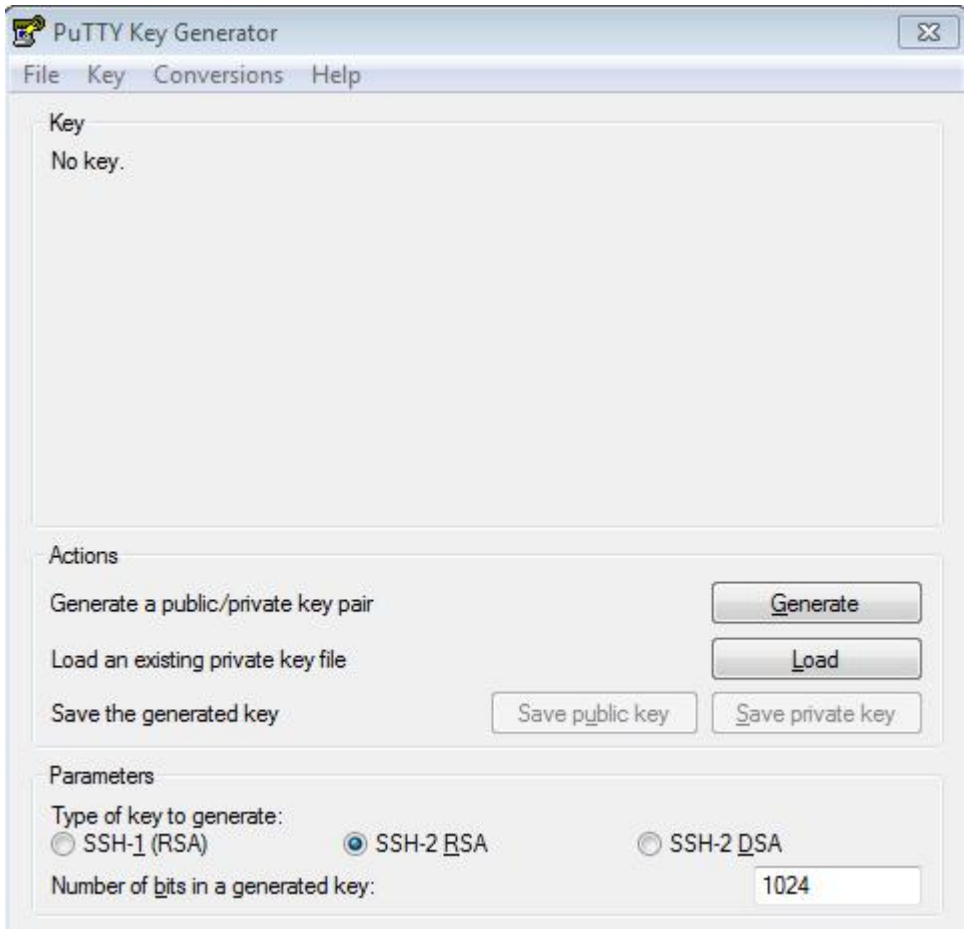
Choose **Security Management**>**Device Administrator**, and add the user name **user** and password **pass**.

Configure the SSH client and set up a connection to the SSH server. For details, see the previous example.

Type in the user name **user** and password **pass**. Verify that you can log in to the SSH server successfully.

```
FS#show users
    Line          User          Host(s)                Idle        Location
   0 con 0                      idle                   00:00:31
* 1 vty 0      user        idle                    00:00:33    192.168.217.60
```

Configuring Public Key Authentication of SSH Users

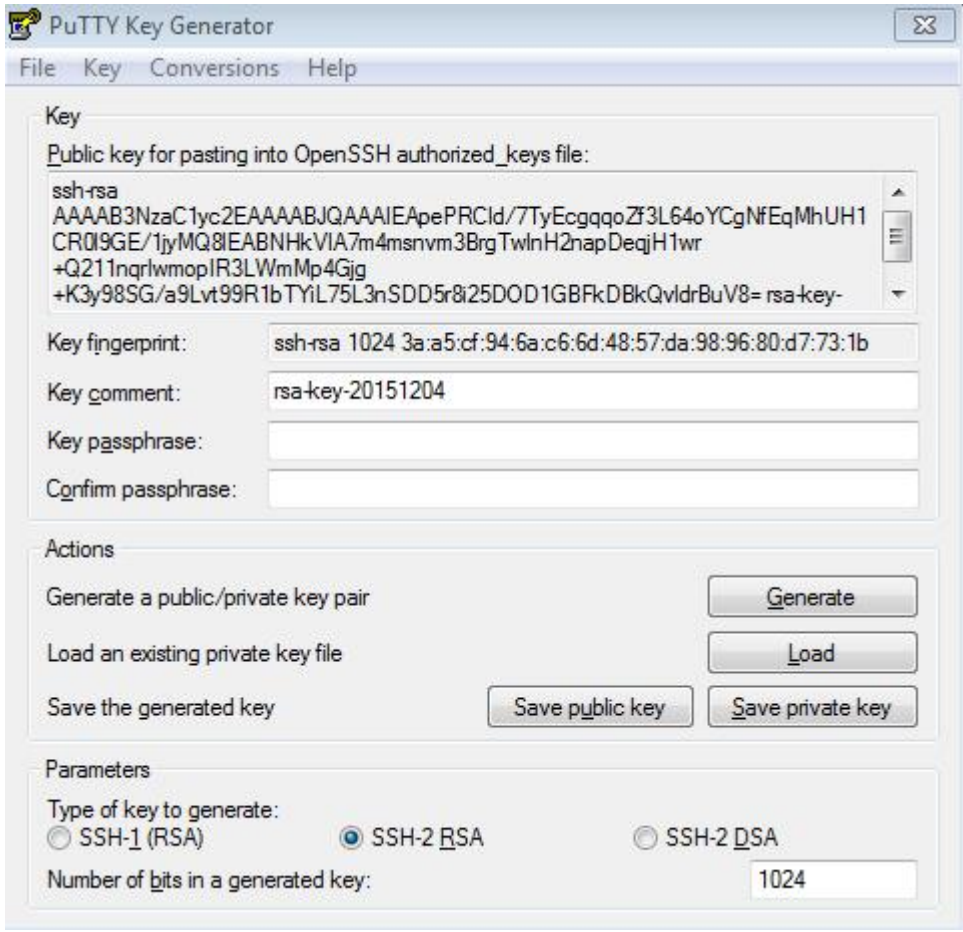
Scenario Figure 4-4-16	 SSH users can use the public key for user authentication, and the public key algorithm is RSA or DSA, as shown in Figure 4-4-16.SSH is configured on the client so that a secure connection is set up between the SSH client and the SSH server.
Configuration Steps	● To implement public key authentication on the client, generate a key pair (for example, RSA key) on the client, place the public key on the SSH server, and select the public key authentication mode. After the key pair is generated on the client, you must save and upload the public key file to the server and complete the server-related settings before you can continue to configure the client and connect the client with the server. ● After the key is generated on the client, copy the public key file from the client to the flash of the SSH server, and associate the file with an SSH user name. A user can be associated with one RSA public key and one DSA public key.
SSH Client	Run the **puttygen.exe** software on the client. Select **SSH-2 RSA** in the **Parameters** pane, and click **Generate** to generate a key, as shown in Figure 4-4-17. Figure 4-4-17 

When a key is being generated, you need to constantly move the mouse over a blank area outside the green progress bar; otherwise, the progress bar does not move and key generation stops, as shown in Figure 4-4-18.

Figure 4-4-18

To ensure security of the RSA public key authentication, the length of the generated RSA key pair must be equal to or larger than 768 bits. In this example, the length is set to 1024 bits.

Figure 4-4-19

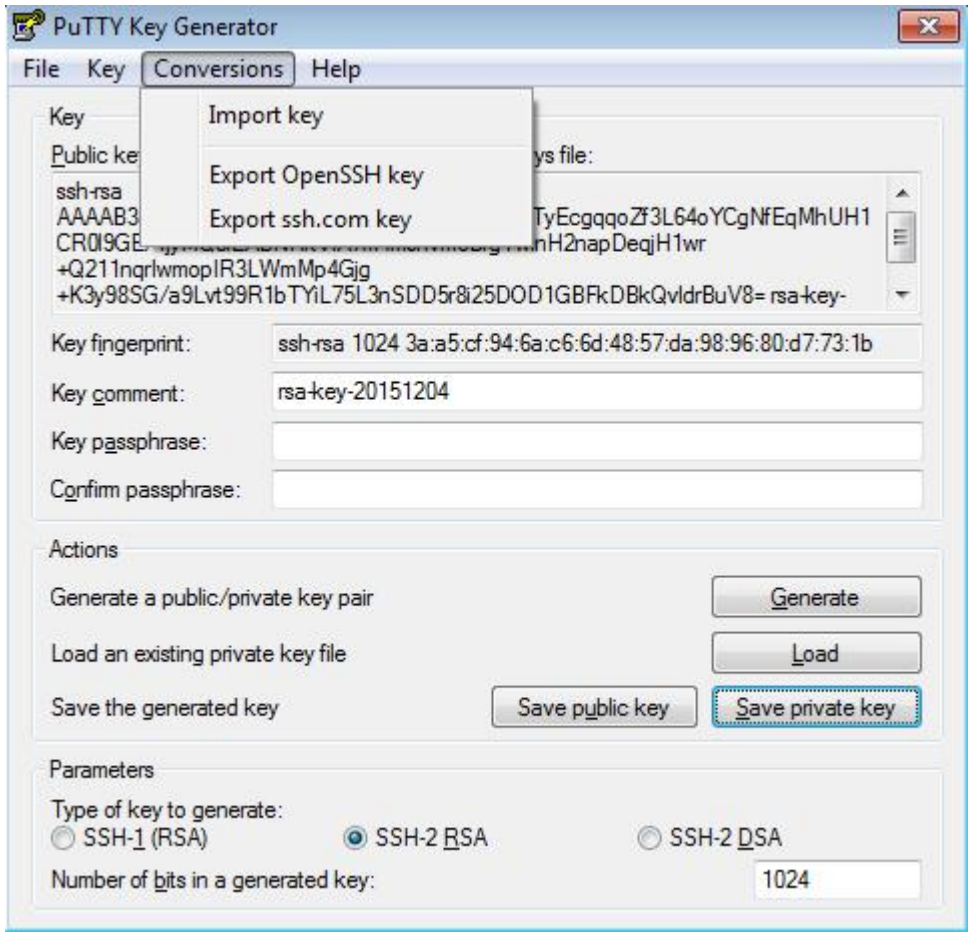


After the key pair is generated, click **Save public key**, type in the public key name **test_key.pub**, select the storage path, and click **Save**. Then click **Save private key**. The following prompt box is displayed. Select **Yes**, type in the public key name **test_private**, and click **Save**.

Figure 4-4-20

You must select the OpenSSH key file; otherwise, the key file cannot be used. The **puttygen.exe** software can be used to generate a key file in OpenSSH format, but this file cannot be directly used by the PuTTY client. You must use **puttygen.exe** to convert the private key to the PuTTY format. Format conversion is not required for the public key file stored on the server, and the format of this file is still OpenSSH, as shown in Figure 4-4-19.

Figure 4-21



SSH Server	FS#configure terminal FS(config)# ip ssh peer test public-key rsaflash:test_key.pub
Verification	● After completing the basic configurations of the client and the server, specify the private key file **test_private** on the PuTTY client, and set the host IP address to **192.168.23.122** and port ID to **22** to set up a connection between the client and the server. In this way, the client can use the public key authentication mode to log in to the network device.
	Figure 4-4-22

Common Errors

- The **no crypto key generate** command is used to delete a key.

4.4.2 Configuring the SCP Service

Configuration Effect

After the SCP function is enabled on a network device, you can directly download files from the network device and upload local files to the network device. In addition, all interactive data is encrypted, featuring authentication and security.

Notes

- The SSH server must be enabled in advance.

Configuration Steps

Enabling the SCP Server

- Mandatory.
- By default, the SCP server function is disabled. Run the **ip scp server enable** command to enable the SCP server function in global configuration mode.

Verification

Run the **show ip ssh** command to check whether the SCP server function is enabled.

Related Commands

Enabling the SCP Server

Command	**ip scp server enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This command is used to enable the SCP server. Run the **no ip scp server enable** command to disable the SCP server.

Configuration Example

Enabling the SCP Server

Configuration Steps	● Run the **ip scp server enable** command to enable the SCP server.
	FS#configure terminal FS(config)#ip scp server enable
Verification	● Run the **show ip ssh** command to check whether the SCP server function is enabled.
	FS(config)#show ipssh SSH Enable - version 1.99 Authentication timeout: 120 secs Authentication retries: 3 SSH SCP Server: enabled

Configuring SSH File Transfer

Scenario Figure 4-4-23	 The SCP service is enabled on the server, and SCP commands are used on the client to transfer data to the server.
Configuration Steps	● Enable the SCP service on the server. The SCP server uses SSH threading. When connecting to a network device for SCP transmission, the client occupies a VTY session (You can finds out that the user type is SSH by running the show user command). ● On the client, use SCP commands to upload files to the server, or download files from the server.

	Syntax of the SCP command: scp [-1246BCpqrv] [-c cipher] [-F ssh_config] [-iidentity_file] [-l limit] [-o ssh_option] [-P port] [-S program] [[user@]host1:]file1 [...] [[user@]host2:]file2 Descriptions of some options: -1: Uses SSHv1 (If not specified, SSHv2 is used by default); -2: Uses SSHv2 (by default); -C: Uses compressed transmission. -c: Specifies the encryption algorithm to be used. -r:Transmits the whole directory; -i: Specifies the key file to be used. -l: Limits the transmission speed (unit: Kbit/s). For other parameters, see the filescp.0. Most options are related to terminals. Few options are supported on both terminals and servers. FS's SCP servers do not support d-p-q-r options. When these options are applied, there are prompts.
SSH Server	FS#configure terminal FS(config)# ip scp server enable
Verification	● File transmission example on the Ubuntu 7.10 system: Set the username of a client to **test** and copy the **config.text** file from the network device with the IP address of 192.168.195.188 to the **/root** directory on the local device.
	root@dhcpd:~#scp test@192.168.23.122:/config.text /root/config.text test@192.168.195.188's password: config.text 100% 1506 1.5KB/s 00:00 Read from remote host 192.168.195.188: Connection reset by peer

4.5 Monitoring

Displaying

Description	Command
Displays the effective SSH server configurations.	**show ipssh**
Displays the established SSH connection.	**show ssh**
Displays the public information of the SSH public key.	**show crypto key mypubkey**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs SSH sessions.	**debug ssh**

5 Configuring DHCP Snooping

5.1 Overview

DHCP Snooping: DHCP Snooping snoops DHCP interactive packets between clients and servers to record and monitor users' IP addresses and filter out illegal DHCP packets, including client request packets and server response packets. The legal user database generated from DHCP Snooping records may serve security applications like IP Source Guard.

Protocols and Standards

- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2132: DHCP Options and BOOTP Vendor Extensions

5.2 Applications

Application	Description
Guarding Against DHCP Service Spoofing	In a network with multiple DHCP servers, DHCP clients are allowed to obtain network configurations only from legal DHCP servers.
Guarding Against DHCP Packet Flooding	Malicious network users may frequently send DHCP request packets.
Guarding Against Forged DHCP Packets	Malicious network users may send forged DHCP request packets, for example, DHCP-RELEASE packets.
Guarding Against IP/MAC Spoofing	Malicious network users may send forged IP packets, for example, tampered source address fields of packets.
Preventing Lease of IP Addresses	Network users may lease IP addresses rather than obtaining them from a DHCP server.
Detecting ARP Attack	Malicious users forge ARP response packets to intercept packets during normal users' communication.

5.2.1 Guarding Against DHCP Service Spoofing

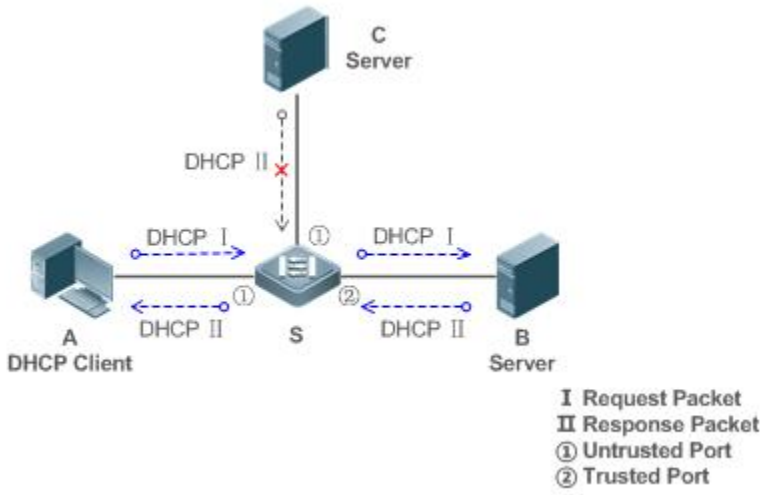
Scenario

Multiple DHCP servers may exist in a network. It is essential to ensure that user PCs obtain network configurations only from the DHCP servers within a controlled area.

Take the following figure as an example. The DHCP client can only communicate with trusted DHCP servers.

- Request packets from the DHCP client can be transmitted only to trusted DHCP servers.
- Only the response packets from trusted DHCP servers can be transmitted to the client.

Figure 5-1



Remarks:	S is an access device. A is a user PC. B is a DHCP server within the controlled area. C is a DHCP server out of the controlled area.

Deployment

- Enable DHCP Snooping on S to realize DHCP packet monitoring.
- Set the port on S connecting to B as trusted to transfer response packets.
- Set the rest of ports on S as untrusted to filter response packets.

5.2.2 Guarding Against DHCP Packet Flooding

Scenario

Potential malicious DHCP clients in a network may send high-rate DHCP packets. As a result, legitimate users cannot obtain IP addresses, and access devices are highly loaded or even break down. It is necessary to take actions to ensure network stability.

With the DHCP Snooping rate limit function for DHCP packets, a DHCP client can only send DHCP request packets at a rate below the limit.

- The request packets from a DHCP client are sent at a rate below the limit.
- Packets sent at rates beyond the limit will be discarded.
- Enable DHCP Snooping correlation with ARP, and delete the non-existing entries.

Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Limit the rates of DHCP packets from the untrusted ports.
- Enable DHCP Snooping correlation with ARP, and detect whether the user is online.

5.2.3 Guarding Against Forged DHCP Packets

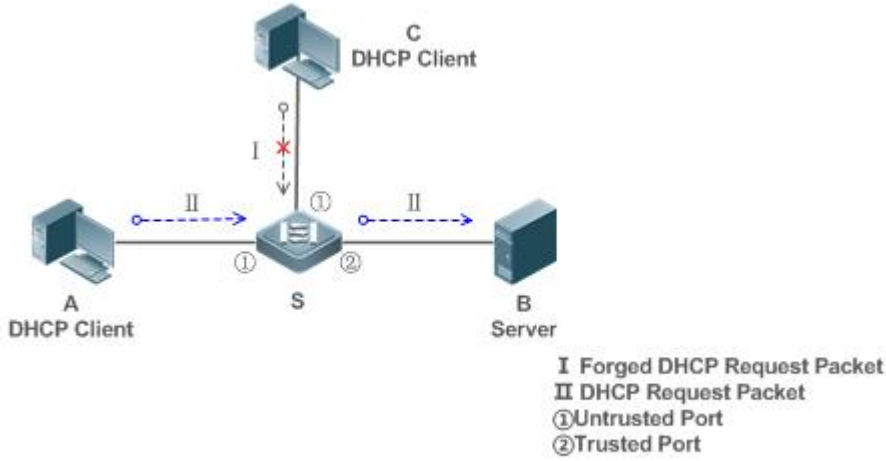
Scenario

Potential malicious clients in a network may forge DHCP request packets, consuming applicable IP addresses from the servers and probably preempting legal users' IP addresses. Therefore, it is necessary to filter out illegal DHCP packets.

For example, as shown in the figure below, the DHCP request packets sent from DHCP clients will be checked.

- The source MAC address fields of the request packets from DHCP clients must match the **chaddr** fields of DHCP packets.
- The Release packets and Decline packets from clients must match the entries in the DHCP Snooping binding database.

Figure 5-2



Remarks:	S is an access device. A and C are user PCs. B is a DHCP server within the controlled area.

Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Set the port on S connecting to B as trusted to transfer response packets.
- Set the rest of ports on S as untrusted to filter response packets.
- Enable DHCP Snooping Source MAC Verification on untrusted ports of S to filter out illegal packets.

5.2.4 Guarding Against IP/MAC Spoofing

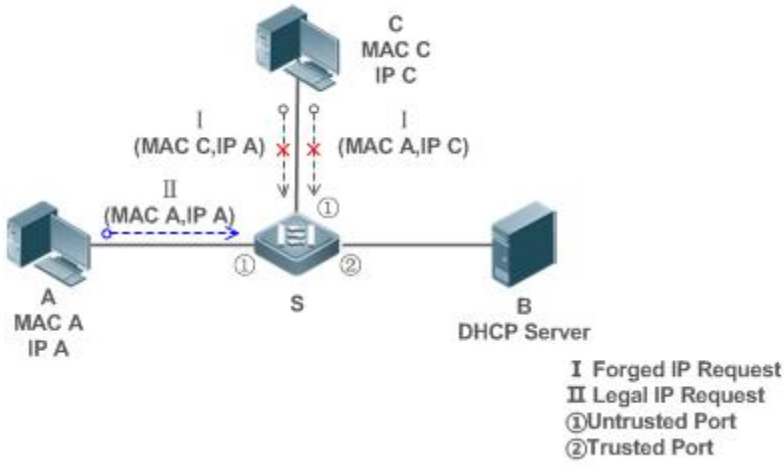
Scenario

Check IP packets from untrusted ports to filter out forged IP packets based on IP or IP-MAC fields.

For example, in the following figure, the IP packets sent by DHCP clients are validated.

- The source IP address fields of IP packets must match the IP addresses assigned by DHCP.
- The source MAC address fields of layer-2 packets must match the **chaddr** fields in DHCP request packets from clients.

Figure 5-3



Remarks:	S is an access device. A and C are user PCs. B is a DHCP server within the controlled area.

Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Set all downlink ports on the S as DHCP Snooping untrusted.
- Enable IP Source Guard on S to filter IP packets.
- Enable IP Source Guard in IP-MAC based mode to check the source MAC and IP address fields of IP packets.

5.2.5 Preventing Lease of IP Addresses

Scenario

Validate the source addresses of IP packets from untrusted ports compared with DHCP-assigned addresses.

If the source addresses, connected ports, and layer-2 source MAC addresses of ports in IP packets do not match the assignments of the DHCP server, such packets will be discarded.

The networking topology scenario is the same as that shown in the previous figure.

Deployment

- The same as that in the section "Guarding Against IP/MAC Spoofing".

5.2.6 Detecting ARP Attacks

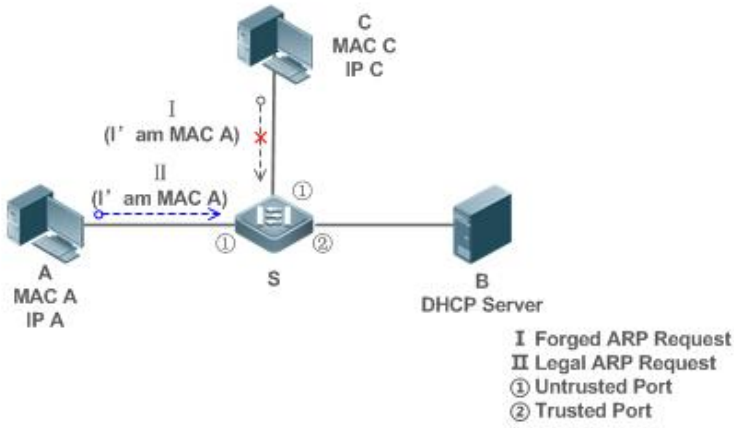
Scenario

Check the ARP packets from untrusted ports and filter out the ARP packets unmatched with the assignments of the DHCP server.

For example, in the following figure, the ARP packets sent from DHCP clients will be checked.

- The ports receiving ARP packets, the layer-2 MAC addresses, and the source MAC addresses of ARP packets senders shall be consistent with the DHCP Snooping histories.

Figure 5-4



Remarks:	S is an access device. A and C are user PCs. B is a DHCP server within the controlled area.

Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Set all downlink ports on the S as untrusted.
- Enable IP Source Guard and ARP Check on all the untrusted ports on S to realize ARP packet filtering.

All the above security control functions are only effective to DHCP Snooping untrusted ports.

5.3 Features

Basic Concepts

DHCP Request Packets

Request packets are sent from a DHCP client to a DHCP server, including DHCP-DISCOVER packets, DHCP-REQUEST packets, DHCP-DECLINE packets, DHCP-RELEASE packets and DHCP-INFORM packets.

DHCP Response Packets

Response packets are sent from a DHCP server to a DHCP client, including DHCP-OFFER packets, DHCP-ACK packets and DHCP-NAK packets.

DHCP Snooping Trusted Ports

IP address request interaction is complete via broadcast. Therefore, illegal DHCP services will influence normal clients' acquisition of IP addresses and lead to service spoofing and stealing. To prevent illegal DHCP services, DHCP Snooping ports are divided into two types: trusted ports and untrusted ports. The access devices only transmit DHCP response packets received on trusted ports, while such packets from untrusted ports are discarded. In this way, we may configure the ports connected to a legal DHCP Server as trusted and the other ports as untrusted to shield illegal DHCP Servers.

On switches, all switching ports or layer-2 aggregate ports are defaulted as untrusted, while trusted ports can be specified. On wireless access points (APs), all the WLAN interfaces are untrusted and cannot be specified as trusted. In fat AP configuration mode, all the layer-2 switching ports and layer-2 encapsulation sub-interfaces are untrusted by default, and can be specified as trusted. In fit AP configuration mode, all the layer-2 switching ports are untrusted by default and can be specified as trusted, and all the layer-2 encapsulation sub-interfaces are trusted and cannot be specified as untrusted. On wireless access controllers (ACs), all WLAN interfaces are untrusted ports and cannot be specified as trusted, and all the switching ports and layer-2 aggregate ports are untrusted ports by default and can be specified as trusted.

DHCP Snooping Packet Suppression

To shield all the DHCP packets on a specific client, we can enable DHCP Snooping packet suppression on its untrusted ports.

VLAN-based DHCP Snooping

DHCP Snooping can work on a VLAN basis. By default, when DHCP Snooping is enabled, it is effective to all the VLANs of the current client. Specify VLANs help control the effective range of DHCP Snooping flexibly.

DHCP Snooping Binding Database

In a DHCP network, clients may set static IP addresses randomly. This increases not only the difficulty of network maintenance but also the possibility that legal clients with IP addresses assigned by the DHCP server may fail to use the network normally due to address conflict. Through snooping packets between clients and servers, DHCP Snooping summarizes the user entries including IP addresses, MAC address, VLAN ID (VID), ports and lease time to build the DHCP Snooping binding database. Combined with ARP detection and ARP check, DHCP Snooping controls the reliable assignment of IP addresses for legal clients.

DHCP Snooping Rate Limit

DHCP Snooping rate limit function can be configured through the rate limit command of Network Foundation Protection Policy (NFPP). For NFPP configuration, see the *Configuring NFPP*.

DHCP Option82

DHCP Option82, an option for DHCP packets, is also called DHCP Relay Agent Information Option. As the option number is 82, it is known as Option82. Option82 is developed to enhance the security of DHCP servers and improve the strategies of IP address assignment. The option is often configured for the DHCP relay

services of a network access device like DHCP Relay and DHCP Snooping. This option is transparent to DHCP clients, and DHCP relay components realize the addition and deduction of the option.

Illegal DHCP Packets

Through DHCP Snooping, validation is performed on the DHCP packets passing through a client. Illegal DHCP packets are discarded, user information is recorded into the DHCP Snooping binding database for further applications (for example, ARP detection). The following types of packets are considered illegal DHCP packets.

- The DHCP response packets received on untrusted ports, including DHCP-ACK, DHCP-NACK and DHCP-OFFER packets
- The DHCP request packets carrying gateway information **giaddr**, which are received on untrusted ports
- When MAC verification is enabled, packets with source MAC addresses different with the value of the **chaddr** field in DHCP packets
- DHCP-RELEASE packets with the entry in the DHCP Snooping binding database Snooping while with untrusted ports inconsistent with settings in this binding database
- DHCP packets in wrong formats, or incomplete

Overview

Feature	Description
Filtering DHCP packets	Perform legality check on DHCP packets and discard illegal packets (see the previous section for the introduction of illegal packets). Transfer requests packets received on trusted ports only.
Building the DHCP Snooping binding database	Snoop the interaction between DHCP clients and the server, and generate the DHCP Snooping binding database to provide basis for other filtering modules.

5.3.1 Filtering DHCP Packets

Perform validation on DHCP packets from untrusted ports. Filter out the illegal packets as introduced in the previous section "Basic Concepts".

Working Principle

During snooping, check the receiving ports and the packet fields of packets to realize packet filtering, and modify the destination ports of packets to realize control of transmit range of the packets.

Checking Ports

In receipt of DHCP packets, a client first judges whether the packet receiving ports are DHCP Snooping trusted ports. If yes, legality check and binding entry addition are skipped, and packets are transferred directly. For not, both the check and addition are needed.

Checking Packet Encapsulation and Length

A client checks whether packets are UDP packets and whether the destination port is 67 or 68. Check whether the packet length match the length field defined in protocols.

Checking Packet Fields and Types

According to the types of illegal packet introduced in the section "Basic Concepts", check the fields **giaddr** and **chaddr** in packets and then check whether the restrictive conditions for the type of the packet are met.

Related Configuration

Enabling Global DHCP Snooping

By default, DHCP Snooping is disabled.

It can be enabled on a device using the **ip dhcp snooping** command.

Global DHCP Snooping must be enabled before VLAN-based DHCP Snooping is applied.

Configuring VLAN-based DHCP Snooping

By default, when global DHCP Snooping is effective, DHCP Snooping is effective to all VLANs.

Use the [**no**] **ip dhcp snooping vlan** command to enable DHCP Snooping on specified VLANs or delete VLANs from the specified VLANs. The value range of the command parameter is the actual range of VLAN numbers.

Configuring DHCP Snooping Source MAC Verification

By default, the layer-2 MAC addresses of packets and the **chaddr** fields of DHCP packets are not verified.

When the **ip dhcp snooping verify mac-address** command is used, the source MAC addresses and the **chaddr** fields of the DHCP request packets sent from untrusted ports are verified. The DHCP request packets with different MAC addresses will be discarded.

5.3.2 Building the Binding Database

DHCP Snooping detects the interactive packets between DHCP clients and the DHCP server, and generate entries of the DHCP Snooping binding database according to the information of legal DHCP packets. All these legal entries are provided to other security modules of a client as the basis of filtering packets from network.

Working Principle

During snooping, the binding database is updated timely based on the types of DHCP packets.

Generating Binding Entries

When a DHCP-ACK packet on a trusted port is snooped, the client's IP address, MAC address, and lease time field are extracted together with the port ID (a wired interface index or a WLAN ID) and VLAN ID. Then, a binding entry of it is generated.

Deleting Binding Entries

When the recorded lease time of a binding entry is due, it will be deleted if a legal DHCP-RELEASE/DHCP-DECLINE packet sent by the client or a DHCP-NCK packet received on a trusted port is snooped, or the **clear** command is used.

Related Configuration

No configuration is needed except enabling DHCP Snooping.

5.4 Configuration

Configuration	Description and Command	
Configuring basic functions of DHCP Snooping	(Mandatory) It is used to enable DHCP Snooping.	
	ip dhcp snooping	Enables DHCP Snooping.
	ip dhcp snooping suppression	Enables DHCP Snooping packet suppression.
	ip dhcp snooping vlan	Enables VLAN-based DHCP Snooping.
	ip dhcp snooping verify mac-address	Configures DHCP Snooping source MAC verification.
	ip dhcp snooping database write-delay	Writes the DHCP Snooping binding database to Flash periodically.
	ip dhcp snooping database write-to-flash	Writes the DHCP Snooping binding database to Flash manually.
	renew ip dhcp snooping database	Imports Flash storage to the DHCP Snooping Binding database.

5.4.1 Configuring Basic Features

Configuration Effect

- Enable DHCP Snooping.
- Generate the DHCP Snooping binding database.
- Control the transmit range of DHCP packets.
- Filter out illegal DHCP packets.

Notes

- The ports on clients connecting a trusted DHCP server must be configured as trusted.
- DHCP Snooping is effective on the wired switching ports, layer-2 aggregate ports, and layer-2 encapsulation sub-interfaces, as well as WLAN interfaces. The configuration can be implemented in interface configuration mode and WLAN security configuration mode.

Configuration Steps

Enabling Global DHCP Snooping

- Mandatory.
- Unless otherwise noted, the feature should be configured on access devices.

Enabling or Disabling VLAN-based DHCP Snooping

- DHCP Snooping can be disabled if not necessary for some VLANs.
- Unless otherwise noted, the feature should be configured on access devices.

Enabling DHCP Snooping Source MAC Validation

- This configuration is required if the **chaddr** fields of DHCP request packets match the layer-2 source MAC addresses of data packets.
- Unless otherwise noted, the feature should be enabled on all the untrusted ports of access devices.

Writing the DHCP Snooping Binding Database to Flash Periodically

- Enable this feature to timely save the DHCP Snooping binding database information in case that client reboot.
- Unless otherwise noted, the feature should be configured on access devices.

Enabling BOOTP Support

- Optional
- Unless otherwise noted, the feature should be configured on access devices.

Enabling DHCP Snooping to Process Relay Requests

- Optional.
- Unless otherwise noted, the feature should be enabled on access devices.

Enabling DHCP Snooping Monitoring

- Optional.
- If DHCP Snooping binding entries need to be generated on a routing port, the feature should be enabled on Layer-3 devices.

Verification

Configure a client to obtain network configurations through the DHCP protocol.

- Check whether the DHCP Snooping Binding database is generated with entries on the client.

Related Commands

Enabling or Disabling DHCP Snooping

Command	[**no**] **ip dhcp snooping**
Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	After global DHCP Snooping is enabled, you can check DHCP Snooping using the **show ip dhcp snooping** command.

Configuring VLAN-based DHCP Snooping

Command	[**no**] **ip dhcp snooping vlan** { *vlan-rng* | {*vlan-min* [*vlan-max*] } }
Parameter Description	*vlan-rng*: Indicates the range of VLANs *vlan-min*: The minimum VLAN ID *vlan-max*: The maximum VLAN ID

Command Mode	Global configuration mode
Usage Guide	Use this command to enable or disable DHCP Snooping on specified VLANs. This feature is available only after global DHCP Snooping is enabled.

Configuring DHCP Snooping Packet Suppression

Command	[**no**] **ip dhcp snooping suppression**
Parameter Description	N/A
Command Mode	Interface configuration mode/WLAN security configuration mode
Usage Guide	Use this command to reject all DHCP request packets at the port, that is, to forbid all users under the port to apply for addresses via DHCP.

Configuring DHCP Snooping Source MAC Verification

Command	[**no**] **ip dhcp snooping verify mac-address**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Through the source MAC address verification, the MAC addresses in link headers and the CLIENT MAC fields in the request packets sent by a DHCP CLIENT are checked for consistence. When the source MAC address verification fails, packets will be discarded.

Writing DHCP Snooping Database to Flash Periodically

Command	[**no**] **ip dhcp snooping database write-delay** [*time*]
Parameter Description	*time*: Indicates the interval between two times of writing the DHCP Snooping database to the Flash.
Command Mode	Global configuration mode
Usage Guide	Use this command to write the DHCP Snooping database to FLASH document. This can avoid binding information loss which requires re-obtaining IP addresses to resume communication after the device restarts.

Writing the DHCP Snooping Database to Flash Manually

Command	**ip dhcp snooping database write-to-flash**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to write the dynamic user information in the DHCP Snooping database in FLASH documents in real time. If a device is upgraded from a non-QinQ version to a QinQ version (or vice versa), binding entries cannot be restored from FLASH documents because of version differences between FLASH documents.

Importing Backep File Storage to the DHCP Snooping Binding Database

Command	**renew ip dhcp snooping database**
Parameter Description	N/A
Command Mode	Privileged configuration mode
Usage Guide	Use this command to import the information from backup file to the DHCP Snooping binding database.

Configure File Backup of the DHCP Snooping Binding Database

Command	**ip dhcp snooping database sata0** [interval *time*]
Parameter Description	*time*: the interval of storing the database in the unit of second. The range is from 10s to 86,400s. The default value is 300s.
Command Mode	Global configuration mode
Usage Guide	After this feature is enabled, the DHCP Snooping database can be written to the backup file of a specified type. In this way, users are able to resume communication immediately after restart of the device.

Enabling or Disabling BOOTP Support

Command	[**no**] **ip dhcp snooping bootp**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to support the BOOPT protocol.

Enabling DHCP Snooping to Process Relay Requests

Command	[**no**] **ip dhcp snooping check-giaddr**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After the feature is enabled, services using DHCP Snooping binding entries generated based on Relay requests, such as IP Source Guard/802.1x authentication, cannot be deployed. Otherwise, users fail to access the Internet. After the feature is enabled, the **ip dhcp snooping verify mac-address** command cannot be used. Otherwise, DHCP Relay requests will be discarded and as a result, users fail to obtain addresses.

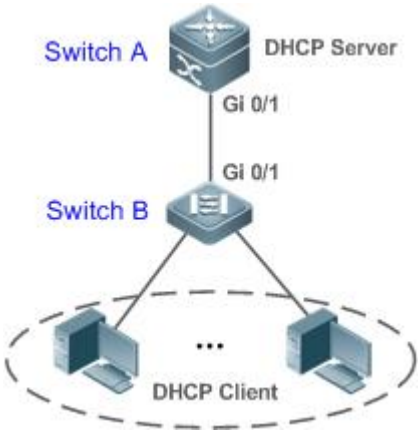
Enabling DHCP Snooping Monitoring

Command	[**no**] **ip dhcp snooping monitor**
Parameter Description	N/A
Command Mode	Global configuration mode

Usage Guide	After the feature is enabled, DHCP Snooping generates binding entries according to the interaction process by copying DHCP packets. It, however, does not check the validity of packets.

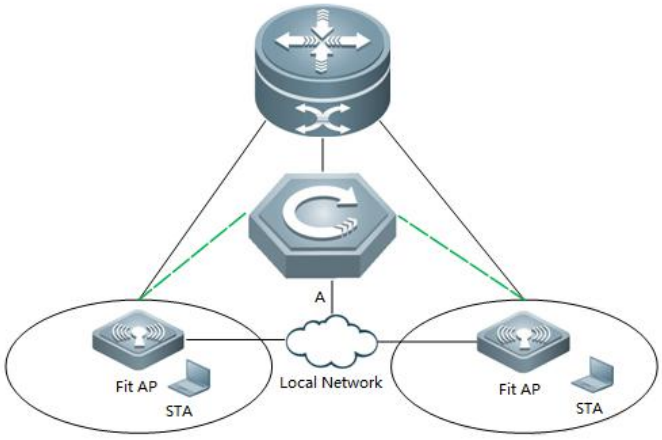
Configuration Example

DHCP Client Obtaining IP addresses Dynamically from a Legal DHCP Server

Scenario Figure 5-5	
Configuration Steps	● Enable DHCP Snooping on an access device (Switch B in this case). ● Configure the uplink port (port Gi 0/1 in this case) as a trusted port.
B	B#configure terminal Enter configuration commands, one per line. End with CNTL/Z. B(config)#ip dhcp snooping B(config)#interface gigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)#ip dhcp snooping trust B(config-if-GigabitEthernet 0/1)#end
Verification	Check the configuration on Switch B. ● Check whether DHCP Snooping is enabled, and whether the configured DHCP Snooping trusted port is uplink. ● Check the DHCP Snooping configuration on Switch B, and especially whether the trusted port is correct.
B	B#show running-config ! ip dhcp snooping ! interface GigabitEthernet 0/1 B#show ip dhcp snooping Switch DHCP Snooping status : ENABLE DHCP Snooping Verification of hwaddr status : DISABLE DHCP Snooping database write-delay time : 0 seconds DHCP Snooping option 82 status : DISABLE DHCP Snooping Support BOOTP bind status : DISABLE Interface Trusted Rate limit (pps) ---------- ------- ---------- GigabitEthernet 0/1 YES unlimited

	B#show ip dhcp snooping binding Total number of bindings: 1 MacAddress IpAddress Lease(sec) Type VLAN Interface ---------- ---------- ---------- ---------- ----- ---------- 0013.2049.9014 172.16.1.2 86207 DHCP-Snooping 1 GigabitEthernet 0/11

Configuring DHCP Snooping for Wireless Fit APs in Local Forwarding Scenarios

Scenario Figure 5- 6	
Configuration Steps	● Configure DHCP Snooping basic functions on the wireless controller.
A	A# configure terminal A(config)# ip dhcp snooping A(config)# end
Verification	Check the DHCP Snooping configuration.
A	A#show ip dhcp snooping Switch DHCP snooping status : ENABLE DHCP snooping Verification of hwaddr status : DISABLE DHCP snooping database write-delay time : 0 seconds DHCP snooping option 82 status : DISABLE DHCP snooping Support bootp bind status : DISABLE Interface Trusted Rate limit (pps) ---------- ------- ---------- Default No unlimited

Common Errors

- The uplink port is not configured as a DHCP trusted port.
- Another access security option is already configured for the uplink port, so that a DHCP trusted port cannot be configured.

5.4.2 Configuring Option82

Configuration Effect

- Enable a DHCP server to obtain more information and assign addresses better.
- The Option82 function is client-oblivious.

Notes

- The Opion82 functions for DHCP Snooping and DHCP Relay are mutually exclusive.

Configuration Steps

- To realize optimization of address allocation, implement the configuration.
- Unless otherwise noted, enable this function on access devices with DHCP Snooping enabled.

Verification

Check whether the DHCP Snooping configuration options are configured successfully.

Related Commands

Adding Option82 to DHCP Request Packets

Command	[**no**] **ip dhcp snooping information option** [**standard-format** | **dot1x-format**]
Parameter Description	**standard-format**: Indicates a standard format of the Option82 options **dot1x-format**: Indicates a dot1x format of the Option82 options
Command Mode	Global configuration mode
Usage Guide	Use this command to add Option82 to DHCP request packets so that a DHCP server assigns addresses according to such information. When dot1x-format is used, if DHCP Relay is configured on the local device and the uplink port connected to the DHCP Server is an SVI port, DHCP Snooping needs to be disabled in the VLAN to which the SVI port belongs.

Configuring Sub-option remote-id of Option82 as User-defined Character String

Command	[**no**] **ip dhcp snooping information option format remote-id** { **string** *ASCII-string* | **hostname** }
Parameter Description	**string** *ASCII-string*: Indicates the content of the extensible format, the Option82 option **remote-id**, is a user-defined character string **hostname**: Indicates the content of the extensible format, the Option82 option **remote-id**, is a host name.
Configuration mode	Global configuration mode
Usage Guide	Use this command to configure the sub-option **remote-id** of the Option82 as user-defined content, which is added to DHCP request packets. A DHCP server assigns addresses according to Option82 information.

Configuring Sub-Option circuit -id of Option82 as User-defined Character String

Command	[**no**] **ip dhcp snooping vlan** *vlan-id* **information option format-type circuit-id string** *ascii-string*
Parameter Description	*vlan-id*: Indicates the VLAN where a DHCP request packet is *ascii-string*: Indicates the user-defined string

Configuration mode	Interface configuration mode
Usage Guide	Use this command to configure the sub-option **circuit-id** of the Option82 as user-defined content, which is added to DHCP request packets. A DHCP server assigns addresses according to Option82 information.

Configuration Example

Configuring Option82 to DHCP Request Packets

Configuration Steps	● Configuring basic functions of DHCP Snooping. ● Configuring Option82.
B	FS# configure terminal FS(config)# ip dhcp snooping information option FS(config)# end
Verification	Check the DHCP Snooping configuration.
B	B#show ip dhcp snooping Switch DHCP Snooping status : ENABLE DHCP Snooping Verification of hwaddr status : DISABLE DHCP Snooping database write-delay time : 0 seconds DHCP Snooping option 82 status : ENABLE DHCP Snooping Support bootp bind status : DISABLE Interface Trusted Rate limit (pps) ---------- ------- ---------- GigabitEthernet 0/1 YES unlimited

Common Errors

- N/A

5.5 Monitoring

Clearing

Running the clear commands may lose vital information and thus interrupt services.

Description	Command
Clears the DHCP Snooping binding database.	**clear ip dhcp snooping binding** [*ip*] [*mac*] [**vlan** *vlan-id*] [**interface** *interface-id* | **wlan** *wlan-id*]
Clears dynamic user inforamtion of DHCP Snooping database.	**clear ip dhcp snooping binding** [*ip*] [*mac*] [**vlan** *vlan-id*] [**interface** *interface-id*]

Displaying

Description	Command
Displays DHCP Snooping configuration.	**show ip dhcp snooping**
Displays the DHCP Snooping binding database.	**show ip dhcp snooping binding**

Debugging

System resources are occupied when debugging information is output. Disable the debugging switch immediately after use.

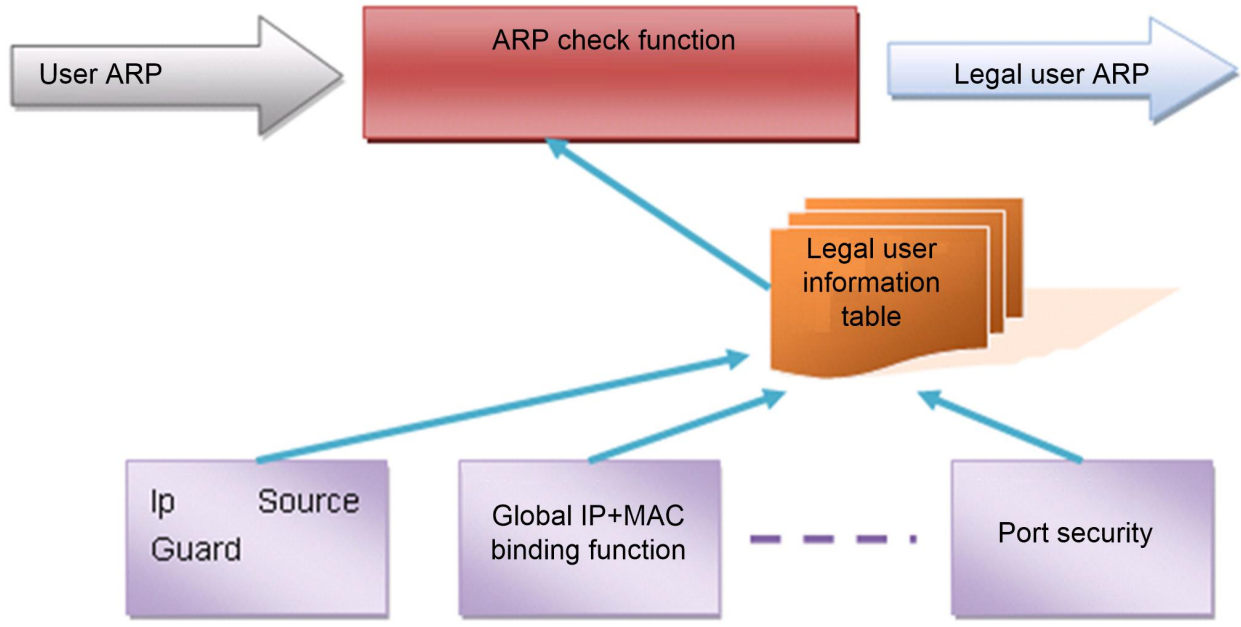
Description	Command
Debugs DHCP Snooping events.	**debug snooping ipv4 event**
Disables debugging DHCP Snooping events.	**no debug snooping ipv4 event**
Debugs DHCP Snooping packets.	**debug snooping ipv4 packet**
Disables debugging DHCP Snooping packets.	**no debug snooping ipv4 packet**
Enables debugging MAC-based DHCP Snooping.	**debug snooping ipv4 mac-address** *H.H.H*
Disables debugging MAC-based DHCP Snooping.	**no debug snooping ipv4 mac-address** *H.H.H*
Enables debugging all DHCP Snooping	**debug snooping ipv4 all**
Disables debugging all DHCP Snooping	**no debug snooping ipv4 all**

6 Configuring ARP Check

6.1 Overview

The Address Resolution Protocol (ARP) packet check filters all ARP packets under ports (including wired layer-2 switching ports, layer-2 aggregate ports (APs), and layer-2 encapsulation sub-interfaces, as well as WLAN interfaces) and discards illegal ARP packets, so as to effectively prevent ARP deception via networks and to promote network stability. On devices supporting ARP check, illegal ARP packets in networks will be ignored according to the legal user information (IP-based or IP-MAC based) generated by security application modules such as IP Source Guard, global IP+MAC binding, 802.1X authentication, GSN binding, Web authentication and port security.

Figure 6-1



The above figure shows that security modules generate legal user information (IP-based or IP-MAC based). ARP Check uses the information to detect whether the Sender IP fields or the <Sender IP, Sender MAC>fields in all ARP packets at ports matches those in the list of legal user information. If not, all unlisted ARP packets will be discarded.

Protocols and Standards

- RFC826: An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses

6.2 Applications

Application	Description
Filtering ARP packets in Networks	Illegal users in networks launch attacks using forged ARP packets.

6.2.1 Filtering ARP Packets in Networks

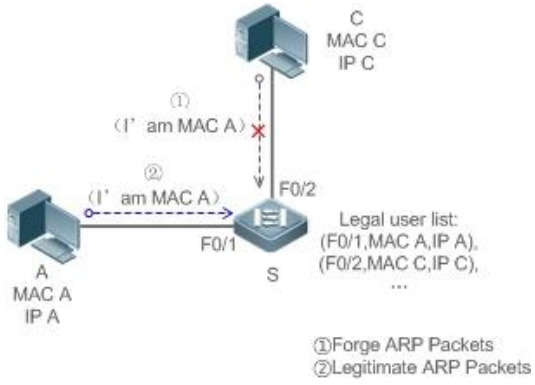
Scenario

Check ARP packets from distrusted ports and filter out ARP packets with addresses not matching the results assigned by the DHCP server.

For example, in the following figure, the ARP packets sent by DHCP clients are checked.

- The ports receiving ARP packets, the source MAC addresses of ARP packets, and the source IP addresses of ARP packets shall be consistent with the snooped DHCP-assigned records.

Figure 6-2



Remarks:	S is an access device. A and C are user PCs.

Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Set all the downlink ports on S as DHCP distrusted ports.
- Enable IP Source Guard and ARP Check on all distrusted ports on S to realize ARP packet filtration.

6.3 Features

Basic Concepts

↘ Compatible Security Modules

Presently, the ARP Check supports the following security modules.

- IP-based: IP-based mode: port security, and static configuration of IP Source Guard.
- IP-MAC based: IP-MAC based mode: port security, global IP+MAC binding, 802.1X authorization, IP Source Guard, GSN binding, and Web authentication.

↘ Two Modes of APR Check

The ARP Check has two modes: Enabled and Disabled. The default is Enabled.

16. Enabled Mode

Through ARP Check, ARP packets are detected based on the IP/IP-MAC based binding information provided by the following modules.

- Global IP-MAC binding
- 802.1X authorization
- IP Source Guard
- GSN binding
- Port security
- Web authentication
- Port security IP+MAC binding or IP binding

When only ARP Check is enabled on a port but the above-mentioned modules are not enabled, legal user information cannot be generated, and thereby all ARP packets from this port will be discarded.

When the ARP Check and VRRP functions are enabled on an interface, if the physical IP address and virtual IP address of the interface can be used as the gateway address, the physical IP address and VRRP IP address need to be permitted to pass. Otherwise, ARP packets sent to the gateway will be filtered out.

17. Disabled Mode

ARP packets on a port are not checked.

Overview

Feature	Description
Filtering ARP Packets	Check the source IP and source MAC addresses of ARP packets to filter out illegal ARP packets.

6.3.1 Filtering ARP Packets

Enable ARP Check on specified ports to realize filtration of illegal ARP packets.

Working Principle

A device matches the source IP and source MAC addresses of the ARP packets received at its ports with the legal user information of the device. With successful matching, packets will be transferred, or otherwise they will be discarded.

Related Configuration

Enabling ARP Check on Ports

By default, the ARP Check is disabled on ports.

Use the **arp-check** command to enable ARP Check.

Unless otherwise noted, this function is usually configured on the ports of access devices.

6.4 Configuration

Configuration	Description and Command	
Configuring ARP Check	(Mandatory) It is used to enable APR Check.	
	arp-check	Enables ARP Check.

6.4.1 Configuring ARP Check

Configuration Effect

- Illegal ARP packets are filtered out.

Notes

- When ARP Check is enabled, the number of policies or users of related security applications may decrease.
- ARP Check cannot be configured on mirrored destination ports.
- ARP Check cannot be configured on the trusted ports of DHCP Snooping.
- ARP Check cannot be configured on global IP+MAC exclude ports.
- ARP Check can be enabled only on wired switching ports, layer-2 APs, layer-2 encapsulation sub-interfaces, as well as WLAN interfaces. Enable ARP check for the wired in interface configuration mode, while for the wireless in WLAN security configuration mode.
- For fit APs in wired access mode, ARP Check needs to be enabled in ap-config all mode.

Configuration Steps

Enabling ARP Check

- (Mandatory) The function is disabled by default. To use the ARP Check function, an administrator needs to run a command to enable it.

Verification

- Use the **show run** command to display the system configuration.
- Use the **show interfaces** { *interface-type interface-number* } **arp-check list** command to display filtering entries.

Related Commands

Enabling ARP Check

Command	**arp-check**
Parameter Description	N/A
Command	Interface configuration mode, WLAN security configuration mode, or WLAN ap-config all configuration mode
Usage Guide	Generate ARP filtration information according to the legal user information of security

	application modules to filter out illegal ARP packets in networks. When the ARP Check function is enabled in WLAN ap-config all mode, the function is enabled on wired ports of all APs.

Configuration Example

The following configuration example introduces only ARP Check related configurations.

Enabling ARP Check on ports

Configuration Steps	• Enable ARP Check. Restricted ARP packets must conform to entries of IP Source Guard, port security, or global IP+MAC binding.
	FS# configure terminal FS(config)#address-bind 192.168.1.3 00D0.F800.0003 FS(config)#address-bind install FS(config)#ip source binding 00D0.F800.0002 vlan 1 192.168.1.4 interface gigabitEthernet 0/1 FS(config)# interface GigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)#arp-check FS(config-if-GigabitEthernet 0/1)#ip verify source port-security FS(config-if-GigabitEthernet 0/1)#switchport port-security FS(config-if-GigabitEthernet 0/1)#switchport port-security binding 00D0.F800.0001 vlan 1 192.168.1.1 FS(config-if-GigabitEthernet 0/1)#exit FS(config)#interface gigabitEthernet 0/4 FS(config-if-GigabitEthernet 0/4)#switchport port-security FS(config-if-GigabitEthernet 0/4)#switchport port-security binding 192.168.1.5 FS(config-if-GigabitEthernet 0/4)#arp-check FS(config-if-GigabitEthernet 0/4)#exit FS(config)#interface gigabitEthernet 0/5 FS(config-if-GigabitEthernet 0/5)#arp-check FS(config-if-GigabitEthernet 0/5)#end FS# configure terminal FS#conf Enter configuration commands, one per line. End with CNTL/Z. FS(config)# ip source binding 0026.c79f.6e4c vlan 1 172.168.131.1 wlan 1
Verification	Use the **show interfaces arp-check list** command to display the effective ARP Check list for interfaces.

Configuration Steps	● Enable ARP Check. Restricted ARP packets must conform to entries of IP Source Guard, port security, or global IP+MAC binding.
	FS# configure terminal FS(config)#address-bind 192.168.1.3 00D0.F800.0003 FS(config)#address-bind install FS(config)#ip source binding 00D0.F800.0002 vlan 1 192.168.1.4 interface gigabitEthernet 0/1 FS(config)# interface GigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)#arp-check FS(config-if-GigabitEthernet 0/1)#ip verify source port-security FS(config-if-GigabitEthernet 0/1)#switchport port-security FS(config-if-GigabitEthernet 0/1)#switchport port-security binding 00D0.F800.0001 vlan 1 192.168.1.1 FS(config-if-GigabitEthernet 0/1)#exit FS(config)#interface gigabitEthernet 0/4 FS(config-if-GigabitEthernet 0/4)#switchport port-security FS(config-if-GigabitEthernet 0/4)#switchport port-security binding 192.168.1.5 FS(config-if-GigabitEthernet 0/4)#arp-check FS(config-if-GigabitEthernet 0/4)#exit FS(config)#interface gigabitEthernet 0/5 FS(config-if-GigabitEthernet 0/5)#arp-check FS(config-if-GigabitEthernet 0/5)#end FS# configure terminal FS#conf Enter configuration commands, one per line. End with CNTL/Z. FS(config)# ip source binding 0026.c79f.6e4c vlan 1 172.168.131.1 wlan 1
Verification	Use the **show interfaces arp-check list** command to display the effective ARP Check list for interfaces.
	FS# show interfaces arp-check list INTERFACE SENDER MAC SENDER IP POLICY SOURCE ---------- ---------- ---------- ---------- GigabitEthernet 0/1 00d0.f800.0003 192.168.1.3 address-bind

Configuration Steps	● Enable ARP Check. Restricted ARP packets must conform to entries of IP Source Guard, port security, or global IP+MAC binding.
	FS# configure terminal FS(config)#address-bind 192.168.1.3 00D0.F800.0003 FS(config)#address-bind install FS(config)#ip source binding 00D0.F800.0002 vlan 1 192.168.1.4 interface gigabitEthernet 0/1 FS(config)# interface GigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)#arp-check FS(config-if-GigabitEthernet 0/1)#ip verify source port-security FS(config-if-GigabitEthernet 0/1)#switchport port-security FS(config-if-GigabitEthernet 0/1)#switchport port-security binding 00D0.F800.0001 vlan 1 192.168.1.1 FS(config-if-GigabitEthernet 0/1)#exit FS(config)#interface gigabitEthernet 0/4 FS(config-if-GigabitEthernet 0/4)#switchport port-security FS(config-if-GigabitEthernet 0/4)#switchport port-security binding 192.168.1.5 FS(config-if-GigabitEthernet 0/4)#arp-check FS(config-if-GigabitEthernet 0/4)#exit FS(config)#interface gigabitEthernet 0/5 FS(config-if-GigabitEthernet 0/5)#arp-check FS(config-if-GigabitEthernet 0/5)#end FS# configure terminal FS#conf Enter configuration commands, one per line. End with CNTL/Z. FS(config)# ip source binding 0026.c79f.6e4c vlan 1 172.168.131.1 wlan 1
Verification	Use the **show interfaces arp-check list** command to display the effective ARP Check list for interfaces.
	GigabitEthernet 0/1 00d0.f800.0001 192.168.1.1 port-security GigabitEthernet 0/1 00d0.f800.0002 192.168.1.4 DHCP snooping GigabitEthernet 0/4 00d0.f800.0003 192.168.1.3 address-bind GigabitEthernet 0/4 192.168.1.5 port-security GigabitEthernet 0/5 00d0.f800.0003 192.168.1.3 address-bind

Common Errors

- If ARP packets at a port need to be checked but APR-Check is disabled, then APR-Check will not be effective.

6.5 Monitoring

Displaying

Description	Command
Displays the effective ARP Check list based on ports.	**show interfaces** [*interface-type interface-number*] **arp-checklist**
Displays the effective ARP Check list based on WLAN.	**show wlan** [*wlan-id*] **arp-checklist**

7 Configuring IP Source Guard

7.1 Overview

The IP Source Guard function realizes hardware-based IP packet filtering to ensure that only the users having their information in the binding database can access networks normally, preventing users from forging IP packets.

7.2 Applications

Application	Description
Guarding Against IP/MAC Spoofing Attack	In network environments, users set illegal IP addresses and malicious users launch attacks through forging IP packets.

7.2.1 Guarding Against IP/MAC Spoofing Attack

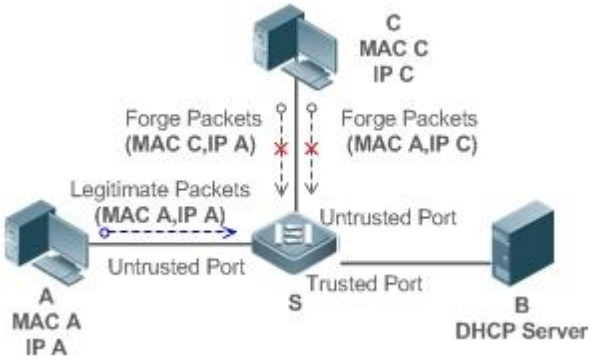
Scenario

Check the IP packets from DHCP untrusted ports. Forged IP packets will be filtered out based on the IP or IP-MAC field.

For example, in the following figure, the IP packets sent by DHCP clients are checked.

- The Source IP Address fields of IP packets should match DHCP-assigned IP addresses.
- The Source MAC Address fields of layer-2 packets should match the MAC addresses in DHCP request packets from clients.

Figure 7-1



Remarks:	S is a network access server (NAS). A and C are user PCs. B is a DHCP server within the control area.

Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Set all downlink ports on S as DHCP untrusted ports.
- Enable IP Source Guard on S to realize IP packet filtering.

- Enable IP–MAC match mode for IP Source Guard on S, filtering IP packets based on IP and MAC addresses.

7.3 Features

Basic Concepts

Source IP Address

Indicate the source IP address field of an IP packet.

Source MAC Address

Indicate the source MAC address field of an IP packet.

IP-based Filtering

Indicate a policy of IP packet filtering, where only the source IP addresses of all IP packets (except DHCP packets) passing through a port are checked. It is the default filtering policy of IP Source Guard.

IP-MAC based Filtering

A policy of IP packet filtering, where both the source IP addresses and source MAC addresses of all IP packets are checked, and only those user packets with these IP addresses and MAC addresses existing in the binding database are permitted.

Address Binding Database

As the basis of security control of the IP Source Guard function, the data in the address binding database comes from two ways: the DHCP Snooping binding database and static configuration. When IP Source Guard is enabled, the data of the DHCP Snooping binding database is synchronized to the address binding database of IP Source Guard, so that IP packets can be filtered strictly through IP Source Guard on a device with DHCP Snooping enabled.

Excluded VLAN

By default, when IP Source Guard is enabled on a port, it is effective to all the VLANs under the port. Users may specify excluded VLANs, within which IP packets are not checked and filtered, which means that such IP packets are not controlled by IP Source Guard. At most 32 excluded VLANs can be specified for a port.

Overview

Feature	Description
Checking Source Address Fields of Packets	Filter the IP packets passing through ports by IP-based or IP-MAC based filtering.

7.3.1 Checking Source Address Fields of Packets

Filter the IP packets passing through ports based on source IP addresses or on both source IP addresses and source MAC addresses to prevent malicious attack by forging packets. When there is no need to check and filter IP packets within a VLAN, an excluded VLAN can be specified to release such packets.

Working Principle

When IP Source Guard is enabled, the source addresses of packets passing through a port will be checked. The port can be a wired switching port, a layer-2 aggregate port (AP), or a layer-2 encapsulation sub-interface, or a WLAN interface. Such packets will pass the port only when the source address fields of the packets match the set of the address binding records generated by DHCP Snooping, or the static configuration set by the administrator. There are two matching modes as below.

IP-based Filtering

Packets are allowed to pass a port only if the source IP address fields of them belong to the address binding database.

IP-MAC Based Filtering

Packets are allowed to pass a port only when both the layer-2 source MAC addresses and layer-3 source IP addresses of them match an entry in the address binding database.

Specifying Excluded VLAN

Packets within such a VLAN are allowed to pass a port without check or filtering.

Related Configuration

Enabling IP Source Guard on a Port

By default, the IP Source Guard is disabled on ports.

It can be enabled using the **ip verify source** command.

Usually IP Source Guard needs to work with DHCP Snooping. Therefore, DHCP Snooping should also be enabled. DHCP Snooping can be enabled at any time on FS devices, either before or after IP Source Guard is enabled.

Configuring a Static Binding

By default, legal users passing IP Source Guard check are all from the binding database of DHCP Snooping.

Bound users can be added using the **ip source binding** command.

Specifying an Excluded VLAN

By default, IP Source Guard is effective to all the VLANs under a port.

Excluded VLANs may be specified which are exempted from IP Source Guard using the **ip verify source exclude-vlan** command.

Excluded VLANs can be specified only after IP Source Guard is enabled on a port. Specified excluded VLANs will be deleted automatically when IP Source Guard is disabled on a port.

The above-mentioned port can be a wired switching port, a layer-2 AP port or a layer-2 encapsulation sub-interface, or a WLAN interface.

7.4 Configuration

Configuration	Description and Command	
Configuring IP Source Guard	(Mandatory) It is used to enable IP Source Guard.	
	ip verify source	Enables IP Source Guard on a port.
	ip source binding	Configures a static binding.
	Ip verify source exclude-vlan	Specifies an excluded VLAN for IP Source Guard.

7.4.1 Configuring IP Source Guard

Configuration Effect

- Check the source IP addresses of input IP packets.

Notes

- When IP Source Guard is enabled, IP packets forwarding may be affected. In general case, IP Source Guard is enabled together with DHCP Snooping.
- IP Source Guard cannot be configured on the trusted ports controlled by DHCP Snooping.
- IP Source Guard cannot be configured on the global IP+MAC exclusive ports.
- IP Source Guard can be configured and enabled only on wired switch ports, Layer-2 AP ports, Layer-2 encapsulation sub-ports and WLAN. In a wired access scenario, it is supposed to be configured in the interface configuration mode. In a wireless access scenario, it is supposed to be configured in the WLAN security configuration mode.
- For a Fit AP in a wired access scenario, IP Source Guard is configured and enabled in WLAN ap-config all configuration mode.

Configuration Steps

- Enable DHCP Snooping.
- Enable IP Source Guard.

Verification

Use the monitoring commands to display the address binding database of IP Source Guard.

Related Commands

Enabling IP Source Guard on a Port

Command	**ip verify source** [**port-security**]
Parameter Description	**port-security**: Enable IP-MAC based filtering.
Command	Interface configuration mode/WLAN security configuration mode/WLAN ap-config all configuration mode
Usage Guide	Detection of users based on IP address or both IP and MAC addresses can be realized by

	enabling IP Source Guard for a port. In the WLAN ap-config all configuration mode, once IP Source Guard is enabled, it works on all wired ports of the AP.

Configuring a Static Binding

Command	ip source binding mac-address { vlan vlan-id } ip-address { interface interface-id | wlan wlan-id | ip-mac | ip-only }
Parameter Description	**mac-address:** The MAC address of a static binding **vlan-id:** The VLAN ID of a static binding. It indicates the outer VLAN ID of a QINQ-termination user. binding. Configure it when QINQ-termination products are in use. **ip-address:** The IP address of a static binding *interface-id*: The Port ID (PID) of a static binding **wlan-id:** WLAN ID of a static binding **ip-mac:** IP-MAC based mode **ip-only:** IP-based mode
Configuration Mode	Global configuration mode
Usage Guide	Through this command, legitimate users can pass IP Source Guard detection instead of being controlled by DHCP. For a Fit AP in a wireless scenario, an AC cannot access static information of users that are connected to a wired port of a wireless AP.

Specifying an Exception VLAN for IP Source Guard

Command	**ip verify source exclude-vlan** *vlan-id*
Parameter Description	**vlan-id:** A VLAN ID exempted from IP Source Guard on a port
Command	Interface configuration mode/WLAN security configuration mode
Usage Guide	By using this command, the specified VLANs under a port where IP Source Guard function is enabled can be exempted from check and filtering.

Configuration Example

Enabling IP Source Guard on Port 1

Configuration Steps	● Enable DHCP Snooping. ● Enable IP Source Guard.
	FS(config)# interface GigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# ip verify source FS(config-if-GigabitEthernet 0/1)# end FS(config)# wlansec 1 FS(config-wlansec)# ip verify source port-security FS(config-wlansec)# end

Verification	Displays the address filtering table of IP Source Guard.
	FS# show ip verify source

Configuring a Static Binding

Configuration Steps	● Enable DHCP Snooping. ● Enable IP Source Guard. ● Configure a static binding.
	FS# configure terminal FS(config)# ip source binding 00d0.f801.0101 vlan 1 192.168.4.243 interface GigabitEthernet 0/3 FS(config)# end
Verification	Displays the address filtering table of IP Source Guard.
	FS# show ip verify source NO. INTERFACE FilterType FilterStatus IPADDRESS MACADDRESS VLAN TYPE ----- ---------- ---------- ---------- ---------- ---------- ---- ---------- 1 GigabitEthernet 0/3 UNSET Inactive-restrict-off 192.168.4.243 00d0.f801.0101 1 Static 2 GigabitEthernet 0/1 IP-ONLY Active Deny-All 3 WLAN 1 IP-MAC Active Deny-All

Specifying an Excluded VLAN

Configuration Steps	● Enable DHCP Snooping. ● Enable IP Source Guard.
	FS(config)# interface GigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# ip verify source FS(config-if-GigabitEthernet 0/1)# ip verify source exclude-vlan 1 FS(config-if)# end FS(config)# wlansec 1 FS(config-wlansec)# ip verify source FS(config-wlansec)# ip verify source exclude-vlan 1 FS(config-wlansec)# end
Verification	Display the configuration of excluded VLANs specified on a port.

Configuration Steps	● Enable DHCP Snooping. ● Enable IP Source Guard.
	FS(config)# interface GigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# ip verify source FS(config-if-GigabitEthernet 0/1)# ip verify source exclude-vlan 1 FS(config-if)# end FS(config)# wlansec 1 FS(config-wlansec)# ip verify source FS(config-wlansec)# ip verify source exclude-vlan 1 FS(config-wlansec)# end
Verification	Display the configuration of excluded VLANs specified on a port.
	FS# show run

Common Errors

- Enable IP Source Guard on a trusted port under DHCP Snooping.
- Specify an excluded VLAN before IP Source Guard is enabled.

7.5 Monitoring

Displaying

Description	Command
Displays the address filtering table of IP Source Guard.	**show ip verify source** [**interface** *interface-id* / **wlan** *wlan-id*]
Displays the address binding database of IP Source Guard.	**show ip source binding**

8 Configuring SEC-VPDN

8.1 Overview

The Virtual Private Dial-up Network (VPDN) is a type of Virtual Private Network (VPN) services based on dialup users. It connects to the Internet in dialup access mode and uses the bearer function of the IP network, in combination with authentication and authorization mechanisms, to establish a secure VPN. This technology develops rapidly with the Internet development. VPDN is applicable to customers that have branches distributed scatteredly and have many mobile users, for example, enterprise users and remote education users. FS products support two types of VPDN tunnels:

- Layer 2 Tunneling Protocol (L2TP) tunnels
- Point-to-Point Tunneling Protocol (PPTP) tunnels

The two VPDN tunnel protocols have their own development history. For their configurations and application descriptions, see the chapters below. PPTP is often applied in Microsoft Windows-based products while L2TP is often used in Cisco network devices. As an industrial standard, L2TP is supported by Windows 2000/XP.

Routers refer to general routing and security gateways in this document unless otherwise specified.

8.2 Applications

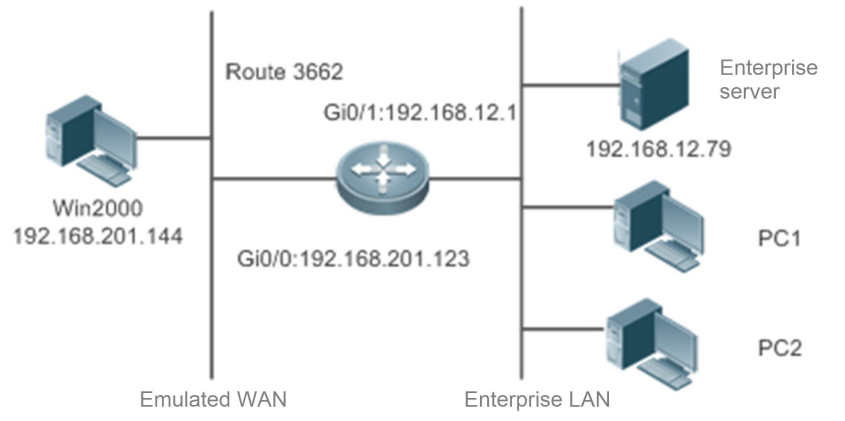
Application	Description
Providing VPDN Dial-in Service	A FS router is as used as an enterprise LAN gateway, and the PPTP protocol is used to provide the VPDN dial-in service.

8.2.1 Providing VPDN Dial-in Service

Scenario

In the network topology shown in Figure 8-1, a FS router is as used as an enterprise Local Area Network (LAN) gateway, and the PPTP protocol is used to provide the VPDN dial-in service. One Windows 2000 PC is used as the VPDN remote client. A PPTP tunnel from the VPDN remote client to FS router is created for accessing the server in the enterprise LAN. Ethernet is deployed between the VPDN remote client and the FS router to simulate the WAN IP network environment for ease of tests. Figure 8-1 shows the relevant IP addresses.

Figure 8-1



Remarks	Routes reachable to remote dial-in users must be configured on LAN servers of the enterprise so that the remote VPDN users can access these LAN servers. In general, the default gateway of these servers needs to be set to the internal gateway address of the router, that is, 192.168.12.1 in this example.

Deployment

- (Optional) Configure a local address pool: Assign IP addresses to clients.
- (Optional) Configure user information: Conduct user identity authentication on clients that attempt to remotely access the local device via PPTP.
- (Mandatory) Configure VPDN global parameters: Configure global parameters.
- (Mandatory) Configure a virtual-template interface. Configure the template of the virtual-access interface for binding and bearing PPTP sessions.
- (Mandatory) Configure a VPDN-group: Set VPDN-group work parameters.

8.3 Features

Basic Concepts

Local Address Pool

If an IP address to be used in a VPN is not set for the remote client, an IP address needs to be assigned to the remote client, so that the router, serving as a PPTP Network Server (PNS), accepts PPTP connections initiated by the remote client. In general, an idle IP address in a specified address pool is assigned to the client.

User Information

User information is optional for the configuration of the PPTP server. User information is used to conduct user identity authentication on clients that attempt to remotely access the local device via PPTP.

VPDN Global Parameters

VPDN global parameters include the following:

- Enable/Disable VPDN: If a router is required to accept the PPTP access from the remote client and establish a PPTP tunnel and session, the VPDN function must be enabled on the router.

- VPDN source address: After the VPDN source address is set, the tunnel destination address set for the remote client must be consistent with the VPDN source address so that a PPTP tunnel is established successfully.
- Maximum VPDN session number: After the maximum VPDN session number is set, an access request will be rejected when the number of existing VPDN sessions reaches the maximum VPDN session number.
- VPDN rate limit: Users can limit the establishment rate of a VPDN tunnel, so as to limit the number of VPDN tunnels that can be established at a time.

Virtual-Template Interface

A virtual-template interface includes the following:

- Virtual-template interface (mandatory): The created virtual-template interface will be used a configuration template of the virtual-access interface for binding and bearing PPTP sessions.
- Local IP address (mandatory)
- Peer IP address (optional)

VPDN-group

A VPDN-group includes the following:

- VPDN-group (mandatory): The destination address in the tunnel establishment request sent from the remote client must match the VPDN-group so that the VPDN-group is applied.
- Tunnel mode (mandatory): Sets whether to accept the dial-in from the remote client. If the local router is required to provide the PNS function, the dial-in from the remote client must be accepted.
- Tunnel protocol (mandatory): Tunnel protocols include L2TP and PPTP. If the local router is required to provide the PNS function, **protocol pptp** or **protocol any** must be set.
- Peer name (optional)
- Local name (optional): If the peer name is set, the VPDN-group is effective only to the remote client that matches the hostname. If no peer name is set, the VPDN-group becomes the default VPDN-group of the system and can provide the VPDN service for any remote client.
- PPTP tunnel parameters (optional): The destination address in the tunnel establishment request sent from the remote client must match the PPTP tunnel parameters so that the VPDN-group is applied.

Maximum VPDN Session Number

Set the maximum number of sessions that are allowed by the VPDN server.

L2TP-Class Interface

An L2TP-class interface includes the following:

- L2TP-class unit: Sets L2TP control connection-relevant parameters. The created L2TP-class interface can be referenced by the pseudowire-class interface by name.
- Maintenance update parameter for L2TP control connections: Sets the transmission interval of Hello messages.

Pseudowire-Class Interface

A Pseudowire-class interface includes the following:

- Pseudowire-class unit: A pseudowire-class unit can be referenced in pseudowire rules of the virtual-PPP interface by name.
- L2TP data transmission encapsulation mode: The data transmission encapsulation mode cannot be changed after it is set. If you need to set L2TP data transmission parameters for the pseudowire-class interface, you must first set the L2TP data transmission encapsulation mode.
- L2TP control connection parameters: The control parameter can be set to L2TPv2. If it is set to L2TPv2, the L2TP protocol that complies with RFC2661 is used to create control connections. The *L2TP-class-name* parameter is used to reference an existing L2TP-class interface to restrict control connection parameters. If the *L2TP-class-name* parameter is not set, the default L2TP control connection parameters of the system are used.

Virtual-PPP Interface

A virtual-ppp interface includes the following:

- Virtual-ppp interface: Creates and binds a specified L2TP session.
- IP address
- Identity authentication parameters: Set the username and password.
- Pseudowire rule: Users can set pseudowire rules for establishing an L2TP session on a virtual-ppp interface. Once pseudowire rules are set for a virtual-PPP interface, the virtual-ppp interface automatically attempts to establish an L2TP session with the specified L2TP Network Server (LNS). If the session fails to established, the virtual-ppp interface re-attempts to establish an L2TP session 10 seconds later.

Overview

Feature	Description
Establishing PPTP Server	Uses PPTP to provide the VPDN dial-in service.
Establishing L2TP Tunnel Initiated by Local Client	Enables a router to serve as an L2TP client to actively initiate negotiation and establish a tunnel with the remote L2TP server.
Establishing L2TP Tunnel Initiated by Remote Client	Enables a router to accept connection requests from the remote L2TP client and negotiate to establish a tunnel.

8.3.1 Establishing PPTP Server

The Point to Point Tunneling Protocol (PPTP) is an enhanced security protocol developed on the basis of the Point to Point Protocol (PPP). It allows using the multiprotocol Virtual Private Network (VPN), Password Authentication Protocol (PAP), and Extensible Authentication Protocol (EAP) to enhance security. PPTP enables remote users to dial in to the Independent Service Provider (ISP) network, directly access the Internet, or use other networks to securely access the enterprise network.

FS products can access the server as a PNS, that is, FS products accept the PPTP tunnel request initiated by the remote client. In this case, the router accepts the connection request from the remote PPTP client and negotiates to establish a tunnel.

Working Principle

PPTP is a network technology that supports multiprotocol VPN. It enables remote users to dial in to the local ISP network by using the Windows NT® Workstation, Windows® 95, Windows® 98, Windows® 2000, and other systems that support the PPP function, so as to span the Internet and securely connect to and access an enterprise network. The PPTP protocol is described in the standard document RFC 2637. It is jointly proposed by Microsoft and several leading communication device developers initially, and is recommended to the Internet Engineering Task Force (IETF) now.

PPTP defines a protocol for transmitting PPP packets via a tunnel in an IP network. It does not revise the PPP protocol but defines a new tool for bearing PPP packets. With the client/server architecture, PPTP has the functions of the Network Access Server (NAS) implemented by the PPTP Network Server (PNS) and PPTP Access Concentrator (PAC) jointly. The PNS is designed to run in universal operating systems in the TCP/IP network, and needs to provide only the IP interface. The PAC generally has one or more physical interfaces that support the Public Switched Telephone Network (PSTN), Integrated Services Digital Network (ISDN) or PPP functions.

FS products can access the server as a PNS, that is, FS products accept the PPTP tunnel request initiated by the remote client. In this case, the router accepts the connection request from the remote PPTP client and negotiates to establish a tunnel.

Related Configuration

Configuring Local Address Pool

Mandatory.

Run the **ip local pool poolname** *first-ip* [*last-ip*] command in global configuration mode to create/set a local address pool.

Run the **no ip local pool** *poolname* command in global configuration mode to delete a specified address pool.

Configuring User Information

Table data, except the daily/weekly/monthly reports, is stored for 60 days by default.

Run the **username user-name password** *password* command to configure user information.

To delete relevant configuration, run the **no username** *user-name* command in global configuration mode.

Configuring VPDN Global Parameters

The historical data of daily reports is stored for 60 days by default.

Perform the following operations to configure VPDN global parameters:

- Enable/Disable VPDN. Run the **vpdn enable** and **no vpdn enable** commands in global configuration mode to enable and disable the VPDN function respectively.

  The operation is mandatory.

- Set/Cancel the VPDN source address. Run the **vpdn source-ip** *ip-address* and **no vpdn source-ip** commands in global configuration mode to set and cancel the VPDN source address respectively.

  By default, the system does not check whether the destination address in the received tunnel establishment request is a specific value.

- Set/Restore the maximum VPDN session number. Run the **vpdn session-limit** *sessions* and **no vpdn session-limit** commands in global configuration mode to set and restore the maximum VPDN session number respectively.

By default, the maximum VPDN session number is the maximum value that can be configured by this command.

- Set the VPDN rate limit. Run the **vpdn limit_rate** *rate_num* command to change the limited connection rate. *rate_num* indicates the number of tunnels that can be established per second. The value ranges from 5 to 100. Run the **no vpdn limit_rate** command to disable the rate limit function.

By default, the rate limit function is enabled. The default rate limit is 15 tunnels per second.

Configuring Virtual-Template Interface

The historical data of weekly reports is stored for 8 weeks by default.

Perform the following operations to configure a virtual-template interface:

- (Mandatory) Set a virtual-template interface.

In global configuration mode, run the **interface virtual-template** *number* command to create/configure a specified virtual -template interface; run the **no interface virtual-template** *number* command to delete a specified virtual- template interface. *number* indicates the serial number of a specified virtual-template interface. The created virtual-template interface will be used as a configuration template of the virtual-access interface for binding and bearing PPTP sessions.

- (Mandatory) Set the local IP address.
- (Optional) Set the identity authentication mode.
- (Optional) Set t the peer IP address.

For details about how to set the local IP address, identity authentication mode, and peer IP address, see the interface configuration guide.

Configuring VPDN-Group

The historical data of monthly reports is stored for 12 months by default.

Perform the following operations to configure a VPDN-group:

- (Mandatory) Set a VPDN-group.

In global configuration mode, run the **vpdn-group** *name* command to create/configure a specified VPDN-group unit; run the **no vpdn-group** *name* command to delete a specified VPDN-group unit. *name* indicates the name of a VPDN-group. The created VPDN-group unit allows a client to access the device and establish a tunnel.

- (Mandatory) Set the tunnel mode.

In config-vpdn configuration mode, run the **accept-dialin** command to accept the dial-in from the remote client; run the **no accept-dialin** command to reject the dial-in from the remote client. If the local router is required to provide the PNS function, the dial-in from the remote client must be accepted.

- (Mandatory) Set the tunnel protocol.

In config-vpdn-acc-in mode, run the **protocol** { any | l2tp | pptp } command to set a tunnel protocol; run the **no protocol** command to cancel the tunnel protocol. The tunnel mode must be set prior to the tunnel protocol. If the local router is required to provide the PNS function, **protocol pptp** or **protocol any** must be configured, and the tunnel mode must be set prior to a tunnel protocol.

- (Mandatory) Set a virtual template.

  In config-vpdn-acc-in mode, run the **virtual-template** *number* command to set a virtual template; run the **no virtual-template** command to cancel referencing a virtual template. Before a virtual template is set for a VPDN-group, the tunnel mode must be set.

- (Optional) Set the peer name.

  In config-vpdn mode: Run the **terminate-from hostname** *name* command to set the name of the peer host. *name* indicates the name of the peer host. Run the **no terminate-from** command to cancel the name of the peer host. If the peer name is set, the VPDN-group is effective only to the remote client that matches the hostname. If no peer name is set, the VPDN-group becomes the default VPDN-group of the system and can provide the VPDN service for any remote client. If no peer name is set for multiple configured VPDN-groups, the system uses the first VPDN-group that meets conditions to accept the dial-in from the remote client.

- (Optional) Set the local name.

  In config-vpdn mode, run the **local name** *name* command to set the local name; run the **no local name** command to cancel the local name. *name* indicates the local name. By default, FS products use the router name as the local name and send the name to the peer host of a tunnel.

- (Optional) Set the VPDN-group source address.

  In config-vpdn mode, run the **source-ip** *src-ip* command to set the VPDN-group source address; run the **no source-ip** command to cancel the VPDN-group source address. *src-ip* indicates the VPDN-group source address. The destination address in the tunnel establishment request sent from the remote client must match the VPDN-group source address so that the VPDN-group is applied.

- (Optional) Set PPTP flow control parameters.

  In config-vpdn mode: Run the **pptp flow-control receive-window** *winsize* command to set the size of the receive window for PPTP sessions. The value ranges from 1 to 64. Run the **no pptp flow-control receive-window** command to cancel the settings of the receive window for PPTP sessions. The size will be restored to the default value, that is, **16** for PAC and **64** for PNS. Run the **pptp flow-control static-rtt** *interval* command to set the static reference time for ACK waiting for packet sending and receiving of PPTP sessions. The value ranges from 100 ms to 5000 ms. Run the **no pptp flow-control static-rtt** command to cancel the static reference time for ACK waiting for packet sending and receiving of PPTP sessions. The value is restored to the default value, that is, **1500** ms. *winsize* indicates the size of the receive window for PPTP sessions and *interval* indicates the static reference time for ACK waiting. For general applications, you do not need to set this parameter and the default value will be used.

- (Optional) Set PPTP tunnel parameters (optional)

  In config-vpdn mode: Run the **pptp tunnel echo** *interval* command to set the interval for a PPTP tunnel to actively send an echo message. The value ranges from 0 seconds to 1000 seconds. Run the **no pptp tunnel echo** command to cancel the transmission interval of a PPTP echo message. The interval is restored to the default value, that is **60** seconds. *interval* indicates the interval for a PPTP tunnel to

actively send an echo message. The value **0** indicates that no echo message is sent actively. When it is set to a value other than **0**, the local device actively sends an echo message to probe the tunnel status if no valid packet is received from the peer end of the tunnel within this interval.

8.3.2 Configuring L2TP

L2TP is a standard Internet tunneling protocol in industry. It has similar functions as the PPTP protocol, for example, it also encrypts network data flows. Their differences are as follows: PPTP requires an IP network while L2TP requires data packet-oriented point-to-point connections; PPTP uses a single tunnel while L2TP uses multiple tunnels; L2TP provides packet header compression and tunnel authentication while PPTP does not.

FS products support L2TP tunnels of two types:

- L2TP tunnels initiated by the local client: A router serves as an L2TP client and actively initiates negotiation to establish a tunnel with the remote L2TP server.
- L2TP tunnels initiated by the remote client: A router accepts the connection request from the remote L2TP client and negotiates to establish a tunnel.

Working Principle

L2TP is a standard tunneling protocol proposed by the IETF by integrating two existing tunneling protocols: Layer 2 Forwarding (L2F) protocol of Cisco and Point-to-Point Tunneling Protocol (PPTP) of Microsoft. The protocol is described in the standard document RFC 2661.

L2TP is an extension to the Point-to-Point Protocol (PPP). It utilizes PPP to implement user identity authentication and data transmission. Different from PPTP, L2TP uses UDP as the protocol for transmitting control messages and data messages.

L2TP is also an important and effective method for implementing VPN. VPN enables both dial-up users and network users who adopt other access modes, to conveniently and securely access internal networks of enterprises.

8.4 Configuration

Configuration	Description and Command	
Configuring PPTP Server	(Mandatory) It is used to provide the VPDN dial-in service via PPTP.	
	ip local pool *poolname first-ip* [*last-ip*]	Creates/Configures a local address pool.
	username *user-name* **password** *password*	Configures user information.
	vpdn congestion_avoidanc	Enables VPDN congestion control.
	vpdn enable	Enables the VPDN function.
	vpdn source-ip *ip-address*	Sets the VPDN source address.
	vpdn session-limit *sessions*	Sets the maximum VPDN session number.

	vpdn limit_rate *rate_num*	Sets the connection rate limit. *rate_num* indicates the number of tunnels that can be established per second. The value ranges from 5 to 100.
	vpdn-group *name*	Creates/Configures a specified VPDN-group unit.
	interface virtual-template *number*	Creates/Configures a specified virtual-template interface.
	accept-dialin	Accepts the dial-in from the remote client.
	protocol { **any** | **l2tp** | **pptp**}	Sets the tunnel protocol.
	virtual-template *number*	Sets a virtual template.
	terminate-from hostname *name*	Sets the peer hostname.
	local name *name*	Sets the local name.
	source-ip *src-ip*	Sets the VPDN-group source address.
	pptp flow-control receive-window *winsize*	Sets the size of the receive window for PPTP sessions. The value ranges from 1 to 64.
	pptp flow-control static-rtt *interval*	Sets the static reference time for ACK waiting for packet sending and receiving of PPTP sessions. The value ranges from 100 to 5,000 ms.
	pptp tunnel echo *interval*	Sets the interval for a PPTP tunnel to actively send echo messages. The value ranges from 0 to 1000 seconds.
Configuring L2TP Tunnel Initiated by Local Client	(Mandatory) It is used to configure an L2TP tunnel initiated by the local client.	
	l2tp-class *l2tp-class-name*	Creates/Configures an L2TP-class interface of a specified name.
	receive-window *size*	Sets the size of the receive window for control connections.
	retransmit { **initial** { **retries** *initial-retries* | **timeout** { **max** | **min** } *initial-timeout* } | **retries** *retries* | **timeout** { **max** | **min** } *timeout* }	Sets the retransmission parameters for control connections.
	timeout setup *seconds*	Sets the maximum time required for establishing a control connection.
	authentication	Configures tunnel identity authentication.

	hostname *host-name*	Configures the local hostname for the control connection.
	password *pass-words*	Sets the tunnel password.
	hello *interval*	Sets the transmission interval of Hello messages.
	pseudowire-class *pseudowire-class-name*	Creates/Configures a pseudowire-class interface of a specified name.
	encapsulation l2tpv2	Sets the data transmission and encapsulation mode.
	ip dfbit set	Forbids tunnel data fragmentation.
	ip ttl *ttl-value*	Sets the TTL for IP headers of the tunnel.
	ip local interface *interface-name*	Specifies the local interface (address) for the tunnel.
	protocol l2tpv2 [*l2tp-class-name*]	Sets the L2TP control connection parameter.
	interface virtual-ppp *number*	Creates/Configures a specified virtual-ppp interface.
	pseudowire *peer-ip-address vcid* {**encapsulation l2tpv2** [**pw-class** *pw-class-name*] | **pw-class** *pw-class-name* }	Sets pseudowire rules.
Configuring L2TP Tunnel Initiated by Remote Client	(Mandatory) It is used to configure an L2TP tunnel initiated by the remote client.	
	ip local pool *poolname first-ip* [*last-Ip*]	Creates/Configures a local address pool.
	username *user-name* **password** { 0 | 7 } *password*	Configures user information.
	vpdn congestion_avoidanc	Enables VPDN congestion control.
	vpdn enable	Enables the VPDN function.
	vpdn source-ip *ip-address*	Sets the VPDN source address.
	vpdn session-limit *sessions*	Sets the maximum VPDN session number.
	vpdn ignore_source	Ignores the source address check on packets from the peer device.

	vpdn limit_rate *rate_num*	Sets the connection rate limit. *rate_num* indicates the number of tunnels that can be established per second. The value ranges from 5 to 100.
	vpdn-group *name*	Creates/Configures a specified VPDN-group unit.
	interface virtual-template *number*	Creates/Configures a specified virtual-template interface.
	accept-dialin	Accepts the dial-in from the remote client.
	protocol { **any** | **l2tp** | **pptp** }	Sets the tunnel protocol.
	virtual-template *number*	Sets a virtual template.
	terminate-from hostname *name*	Sets the peer hostname.
	local name *name*	Sets the local name.
	source-ip *src-ip*	Sets the VPDN-group source address.
	l2tp tunnel authentication	Enables tunnel authentication.
	l2tp tunnel hello *interval*	Sets the transmission interval of Hello messages.
	l2tp tunnel password *pass-word*	Sets the tunnel password.
	l2tp tunnel receive-window *size*	Sets the size of the receive window for tunnel control connections.
	l2tp tunnel retransmit { **retries** *number* | **timeout** { **min** | **max** } *seconds*}	Sets retransmission parameters for tunnel control messages.
	l2tp tunnel timeout { **no-session**| **setup** } *seconds*	Sets the maximum interval for establishing a session connection or control connection of a tunnel.
	l2tp tunnel force_ipsec	Enables the packet encryption check. After this command is configured, only encrypted packets can pass through VPDN tunnels.
	l2tp tunnel avp-hidden-compatible	Supports the RFC2661-compliant AVP Hidden parsing algorithm.
	l2tp ip udp checksum	Sets the UDP checksum to a non-null value.
	ip tos *tos-value*	Sets the IP ToS field.
	ip precedence *value*	Sets the IP precedence field.
	force-local-chap	Forcibly conducts PPP authentication.
	force-local-lcp	Forcibly conducts LCP authentication.
	lcp renegotiation always	Ignores errors occurring in packets from the peer device.

8.4.1 Configuring PPTP Server

Configuration Effect

- Provide the VPDN dial-in service.

Notes

- Enabling/disabling VPDN is mandatory but setting the VPDN source address is optional.
- If the VPDN function is disabled, all existing PPTP tunnels and sessions will be retained but new PPTP tunnels and sessions will not be established.
- The tunnel mode must be set prior to the tunnel protocol. If the local router is required to provide the PNS function, **protocol pptp** or **protocol any** must be configured.
- Before a virtual template is set for a VPDN-group, the tunnel mode must be set.

Configuration Steps

Creating/Configuring Local Address Pool

- Optional.
- If an IP address to be used in a VPN is not set for the remote client, an IP address needs to be assigned to the remote client so that the router, serving as a PNS, accepts PPTP connections initiated by the remote client. In general, an idle IP address in a specified address pool is assigned to the client.

Configuring User Information

- Optional.
- User information is used to conduct user identity authentication on clients that attempt to remotely access the local device via PPTP. The router locally maintains a database that stores names and passwords of users who are allowed to access (dial in to) the local device.

Enabling VPDN Congestion Control

- Optional.
- This option is mandatory if VPDN congestion control needs to be enabled.

Enabling VPDN Function

- Optional.
- If a router is required to accept the PPTP access from the remote client and establish a PPTP tunnel and session, the VPDN function must be enabled on the router.

Setting VPDN Source Address

- Optional.
- After the VPDN source address is set, the tunnel destination address configured for the remote client must be consistent with the VPDN source address so that a PPTP tunnel is successfully established. By default, the system does not check whether the destination address in the received tunnel establishment request is a specific value.

Setting Maximum VPDN Session Number

- Optional.
- After the maximum VPDN session number is set, an access request will be rejected if the number of existing VPDN sessions reaches the maximum value. By default, the maximum session number is the maximum value configured by this command.

Enabling Rate Limit Function

- Optional.
- Limit the establishment rate of VPDN tunnels so as to limit the number of VPDN tunnels that can be established at a time. By default, the rate limit function is disabled.

Creating/Configuring Specified Virtual-Template Interface

- Mandatory.
- The created virtual-template interface will be used as a configuration template of the virtual-access interface for binding and bearing PPTP sessions.

Creating/Configuring Specified VPDN-Group Unit

- Mandatory.
- The created VPDN-group unit allows a client to access and establish a tunnel.

Accepting Remote Client Dial-in

- Optional.
- If the local router needs to provide the PNS function, the dial-in from the remote client must be accepted.

Setting Tunnel Protocol

- Mandatory.
- The tunnel mode must be set prior to the tunnel protocol. If the local router is required to provide the PNS function, protocol pptp or protocol any must be configured.

Setting Virtual Template

- Mandatory.
- Before a virtual template is set for a VPDN-group, the tunnel mode must be set.

Setting Peer Hostname

- Optional.
- If the peer name is set, the VPDN-group is effective only to the remote client that matches the hostname. If no peer name is set, the VPDN-group becomes the default VPDN-group of the system and can provide the VPDN service for any remote client. If no peer name is set for multiple configured VPDN-groups, the system uses the first VPDN-group that meets conditions to accept the dial-in from the remote client.

Setting Local Name

- Optional.
- Set the local name. The local name will be used as a recording attribute and sent to the peer device. By default, FS products use the router name as the local name and send it to the peer host of a tunnel.

Setting VPDN-Group Source Address

- Mandatory.
- The destination address in the tunnel establishment request sent from the remote client must match the VPDN-group source address so that the VPDN-group is applied.

Setting Size of the Receive Window for PPTP Sessions

- Optional.
- Set a PPTP flow control parameter. In general applications, you do not need to set this parameter and the default value will be used.

Setting Static Reference Time for ACK Waiting for Packet Sending and Receiving of PPTP Sessions

- Optional.
- Set a PPTP flow control parameter. In general applications, you do not need to set this parameter and the default value will be used.

Setting Interval for PPTP Tunnel to Actively Send Echo Messages

- Optional.
- Set a PPTP tunnel parameter. In general applications, you do not need to set this parameter and the default value will be used.

Verification

- Use the VPDN dial-in service. Users should be able to access the server of an enterprise LAN via the VPDN dial-in service.

Related Commands

Creating/Configuring Local Address Pool

Command	**ip local pool** *poolname first-ip [last-ip]*
Parameter Description	*poolname*: Indicates the name of the created/configured local address pool. *first-ip*: Indicates the first address in the range of the local address pool. *last-ip*: Indicates the last address in the range of the local address pool.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring User Information

Command	**username** *user-name* **password** *password*
Parameter Description	*user-name*: Indicates the name of the user who is allowed to dial in. *password*: Indicates the user password.
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling VPDN Function

Command	**vpdn enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Setting VPDN Source Address

Command	**vpdn source-ip** *ip-address*
Parameter Description	*Ip-address*: Indicates the VPDN source address.
Command Mode	Global configuration mode
Usage Guide	N/A

Setting Maximum VPDN Session Number

Command	**vpdn session-limit** *sessions*
Parameter Description	*sessions*: Indicates the maximum VPDN session number.
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling Rate Limit Function

Command	**vpdn limit_rate** *rate_num*
Parameter Description	*rate_num*: Indicates the number of tunnels that can be established per second. The value ranges from 5 to 100.
Command Mode	Global configuration mode
Usage Guide	N/A

Creating/Configuring Specified Virtual-Template Interface

Command	**interface virtual-template** *number*

Parameter Description	*number*: Indicates the serial number of a specified virtual-template interface.
Command Mode	Global configuration mode
Usage Guide	N/A

Creating/Configuring Specified VPDN-Group Unit

Command	**vpdn-group** *name*
Parameter Description	*name*: Indicates the name of a VPDN-group.
Command Mode	Global configuration mode
Usage Guide	N/A

Accepting Remote Client Dial-in

Command	**accept-dialin**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Setting Tunnel Protocol

Command	**protocol** { **any** | **l2tp** | **pptp** }
Parameter Description	N/A
Command Mode	config-vpdn-acc-in mode
Usage Guide	The tunnel mode must be set prior to the tunnel protocol. If the local router is required to provide the PNS function, protocol pptp or protocol any must be configured.

Setting Virtual Template

Command	**virtual-template** *number*
Parameter Description	*number*: Indicates the serial number of a specified virtual-template interface.
Command Mode	config-vpdn-acc-in mode
Usage Guide	N/A

Setting Peer Hostname

Command	**terminate-from hostname** *name*
Parameter	*name*: Indicates the peer hostname.

Description	
Command Mode	config-vpdn mode
Usage Guide	N/A

Setting Local Name

Command	**local name** *name*
Parameter Description	*name*: Indicates the local name.
Command Mode	config-vpdn mode
Usage Guide	N/A

Setting VPDN-Group Source Address

Command	**source-ip** *src-ip*
Parameter Description	*src-ip*: Indicates the VPDN-group source address.
Command Mode	config-vpdn mode
Usage Guide	N/A

Setting Size of Receive Window for PPTP Sessions

Command	**pptp flow-control receive-window** *winsize*
Parameter Description	*winsize*: Indicates the size of the receive window for PPTP sessions.
Command Mode	config-vpdn mode
Usage Guide	N/A

Setting Static Reference Time for ACK Waiting for Packet Sending and Receiving of PPTP Sessions

Command	**pptp flow-control static-rtt** *interval*
Parameter Description	*interval*: Indicates the static reference time for ACK waiting for packet sending and receiving of PPTP sessions. The value ranges from 100 to 5,000 ms.
Command Mode	config-vpdn mode
Usage Guide	N/A

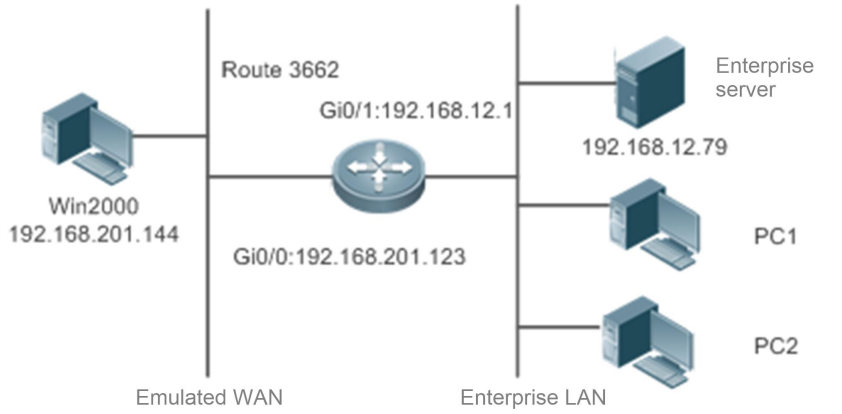
Setting Interval for PPTP Tunnel to Actively Send Echo Messages

Command	**pptp tunnel echo** *interval*
Parameter Description	*interval*: Indicates the interval for a PPTP tunnel to actively send echo messages. The value ranges from 0 to 1000 seconds.
Command	config-vpdn mode

Mode	
Usage Guide	N/A

Configuration Example

Configuring FS Router as Enterprise LAN Gateway and Using PPTP to Provide VPDN Dial-in Service

Scenario **Figure 8-2**	
Configuration Steps	● Configure the FS router as a PPTP server to provide the PPTP dial-in service. Enable the VPDN service. ● Configure a VPDN-group unit, accept the dial-in from the remote client, and set the tunnel protocol to PPTP. ● Configure a local address pool to assign virtual IP addresses to dial-in clients. ● Configure the username and password for client authentication. ● Configure a virtual template, set the PPP authentication mode, and associate the virtual template with the local address pool.
Router	FS # configure terminal FS (config)# vpdn enable FS (config)# vpdn-group pptp FS (config-vpdn)# accept-dialin FS (config-vpdn)# protocol pptp FS (config-vpdn)# virtual-template 1 FS (config)# ip local pool pptp 1.1.1.2 1.1.1.254 FS (config)# username pc password 0 1111 FS (config)# interface Virtual-Template 1 FS (config-if-virtual-template-1)# ppp authentication pap FS (config-if-virtual-template-1)# ip unnumbered FastEthernet 0/1 FS (config-if-virtual-template-1)# peer default ip address pool pptp
Verification	In Windows 2000, in **Network and Dial-up Connections**, create a connection. Select **Connect to a private network through the Internet** in **Network Connection Type**, select **Do not dial the initial connection** in **Public Network**, set the target address to 192.168.201.123, and name the connection **Vpdnconnect**. In the properties of **Vpdnconnect**, set the VPDN server type to PPTP, and define the PAP authentication and optional encryption in security settings. Upon clicking to call, enter the username (**pc**) and password (**1111**) configured for the router. After the configuration is completed, you can dial in to the router from Windows 2000 to

	access the server of the enterprise LAN, for example, the server with the IP address of 192.168.12.79.

8.4.2 Configuring L2TP Tunnel Initiated by Local Client

Configuration Effect

- Enable the local client to initiate an L2TP tunnel. In this case, the router that functions as an L2TP client actively initiates negotiation and establishes a tunnel with the remote L2TP server.

Notes

- The data transmission and encapsulation mode of L2TP tunnels cannot be changed once set. If you need to set L2TP data transmission parameters for the pseudowire-class interface, the L2TP data transmission and encapsulation mode must be set first.
- Users can set pseudowire rules for establishing an L2TP session on the virtual-ppp interface. Once pseudowire rules are set on a virtual-PPP interface, the virtual-ppp interface automatically attempts to establish an L2TP session with a specified LNS. If the session fails to established, the virtual-ppp interface re-attempts to establish an L2TP session 10 seconds later.
- FS products can also use the name of a specified LNS to establish an L2TP session provided that the DNS service is enabled. FS products provide only the DNS client service and the name of the specified LNS must be registered with the DNS server. Once pseudowire rules are set on a virtual-ppp interface, the virtual-ppp interface automatically attempts to establish an L2TP session with the specified LNS. If the session fails to be established, the virtual-ppp interface re-attempts to establish an L2TP session 10 seconds later.

Configuration Steps

↘ **Creating/Configuring L2TP-Class Interface of Specified Name**

- Mandatory.
- *L2TP-class-name* indicates the name of the created/configured L2TP-class unit. The created L2TP-class interface can be referenced by the pseudowire-class interface by name.

↘ **Setting Size of Receive Window for Control Connections**

- Optional.
- Set a time parameter for L2TP control connections. The default size of the receive window is 8.

↘ **Setting Retransmission Parameters for Control Connections**

- Optional.
- Set a time parameter for L2TP control connections. initial-retries indicates the number of SCCRQ retransmission times and the default value is 2; initial-timeout indicates the SCCRQ retransmission interval, the default minimum interval is1 second, and the default maximum interval is 8 seconds; retries indicates the number of retransmission times of control messages, and the default value is 5; timeout indicates the retransmission interval of control messages, the default minimum interval is 1 second, and the default maximum interval is 8 seconds.

Setting Maximum Time Required for Establishing Control Connection

- Optional.
- Set a time parameter for L2TP control connections. Set the upper limit of time required for establishing a control connection (tunnel). The default value is 120 seconds.

Configuring Tunnel Identity Authentication

- Optional.
- By default, FS products do not need tunnel authentication and use the router name as the local hostname. If tunnel authentication is required, the local hostname of a control connection and tunnel password need to be set.

Configuring Local Hostname for Control Connection

- Optional.
- Use the router name as the local hostname.

Setting Tunnel Password

- Optional.
- Set the same tunnel password at both ends.

Setting Transmission Interval of Hello Messages

- Optional.
- Set the transmission interval of Hello messages. The default value is 60 seconds.

Creating/Configuring Pseudowire-Class Interface of Specified Name

- Mandatory.
- The created pseudowire-class interface can be referenced in pseudowire rules of the virtual-PPP interface by name.

Setting Data Transmission and Encapsulation Mode

- Optional.
- The data transmission and encapsulation mode of L2TP tunnels cannot be changed once set. If you need to set L2TP data transmission parameters for the pseudowire-class interface, the L2TP data transmission and encapsulation mode must be set first.

Forbidding Tunnel Data Fragmentation

- Optional.
- Set IP parameters for L2TP data transmission. Setting the IP parameters for L2TP data transmission is actually setting parameters for the IP headers in L2TP UDP messages. By default, the system allows tunnel data fragmentation.

Setting TTL for IP Headers of Tunnel

- Optional.
- Set an IP parameter for L2TP data transmission. The default TTL is 255.

Specifying Local Interface (Address) for Tunnel

- Optional.
- Set an IP parameter for L2TP data transmission. The system sets the local address (interface) nearest to the specified peer address on a route.

Setting L2TP Control Connection Parameter

- Optional.
- L2TPv2 indicates that the L2TP protocol that complies with RFC2661 is used to create control connections. The *L2TP-class-name* parameter is used to reference an existing L2TP-class interface to restrict the control connection parameter. If this parameter is not set, the default L2TP control connection parameter of the system is used.

Creating/Configuring Specified virtual-PPP Interface

- Optional.
- The created virtual-ppp interface will be used to create and bind an L2TP session.

Setting Pseudowire Rules

- Optional.
- You can set pseudowire rules for establishing an L2TP session on the virtual-ppp interface. Once pseudowire rules are set on a virtual-PPP interface, the virtual-ppp interface automatically attempts to establish an L2TP session with a specified LNS. If the session fails to established, the virtual-ppp interface re-attempts to establish an L2TP session 10 seconds later. *peer-ip-address* indicates the address of the remote LNS, *vcid* indicates the global ID, and *pw-class-name* indicates the name of the referenced pseudowire-class interface.

Verification

- Use Cisco 2620 as an L2TP server and FS router as an L2TP client to initiate a connection.

Related Commands

Creating/Configuring L2TP-Class Interface of Specified Name

Command	**l2tp-class** *l2tp-class-name*
Parameter Description	*L2TP-class-name*: Indicates the name of the created/configured L2TP-class unit.
Command Mode	Global configuration mode
Usage Guide	N/A

Setting Size of the Receive Window for Control Connections

Command	**receive-window** *size*

Parameter Description	*size*: Indicates the size of the receive window. The default value is 8.
Command Mode	config-l2tp-class mode
Usage Guide	N/A

Setting Retransmission Parameters for Control Connections

Command	**retransmit** { **initial** { **retries** *initial-retries* | **timeout** { **max** | **min** } *initial-timeout* } | **retries** *retries* | **timeout** { **max** | **min** } *timeout* }
Parameter Description	*initial-retries*: Indicates the number of SCCRQ retransmission times. The default value is 2. *initial-timeout*: Indicates the SCCRQ retransmission interval, the default minimum interval is 1 second, and the default maximum interval is 8 seconds. *retries*: Indicates the number of retransmission times of control messages. The default value is 5. *timeout*: Indicates the retransmission interval of control messages, the default minimum interval is 1 second, and the default maximum interval is 8 seconds.
Command Mode	config-l2tp-class mode
Usage Guide	N/A

Setting Maximum Time Required for Establishing Control Connection

Command	**timeout setup** *seconds*
Parameter Description	*seconds*: Indicates the upper limit of the time required for establishing a control connection (tunnel). The default value is 120 seconds.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Tunnel Identity Authentication

Command	**Authentication**
Parameter Description	N/A
Command Mode	config-l2tp-class mode
Usage Guide	N/A

Configuring Local Hostname for Control Connection

Command	**hostname** *host-name*
Parameter Description	*host-name*: Indicates the local hostname.
Command Mode	config-l2tp-class mode

Usage Guide	N/A

Setting Tunnel Password

Command	**password** *pass-words*
Parameter Description	*pass-words*: Indicates the password for tunnel authentication.
Command Mode	config-l2tp-class mode
Usage Guide	N/A

Setting Transmission Interval of Hello Messages

Command	**hello** *interval*
Parameter Description	*Interval*: Indicates the transmission interval of Hello messages. The default value is 60 seconds.
Command Mode	config-l2tp-class mode
Usage Guide	N/A

Creating/Configuring Pseudowire-Class Interface of Specified Name

Command	**pseudowire-class** *pseudowire-class-name*
Parameter Description	*pseudowire-class-name*: Indicates the name of the created/configured pseudowire-class unit.
Command Mode	Global configuration mode
Usage Guide	N/A

Setting Data Transmission and Encapsulation Mode

Command	**encapsulation l2tpv2**
Parameter Description	N/A
Command Mode	config-pw-class mode
Usage Guide	N/A

Forbidding Tunnel Data Fragmentation

Command	**ip dfbit set**
Parameter Description	N/A
Command Mode	config-pw-class mode
Usage Guide	N/A

Setting TTL for IP Headers for Tunnel

Command	**ip ttl** *ttl-value*
Parameter Description	*ttl-value*: Indicates the TTL of IP headers. The default value is 255.
Command Mode	config-pw-class mode
Usage Guide	N/A

Specifying Local Interface (Address) for Tunnel

Command	**ip local interface** *interface-name*
Parameter Description	*interface-name*: Indicates the local interface of the tunnel. The system sets the local address (interface) nearest to the specified peer address on a route.
Command Mode	config-pw-class mode
Usage Guide	N/A

Setting L2TP Control Connection Parameter

Command	**protocol l2tpv2** [*l2tp-class-name*]
Parameter Description	*l2tp-class-name*: Indicates the name of an existing L2TP-class interface referenced to limit the control connection parameter. If this parameter is not set, the default L2TP control connection parameter of the system is used.
Command Mode	config-pw-class mode
Usage Guide	N/A

Creating/Configuring Specified Virtual-PPP Interface

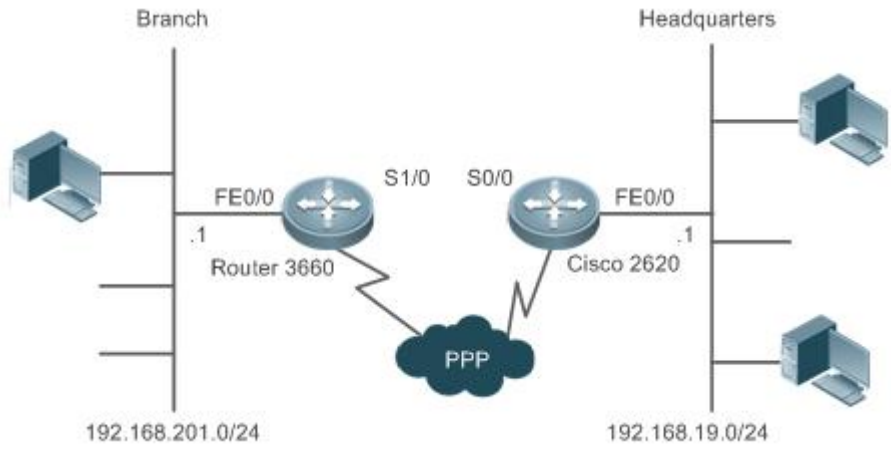
Command	**interface virtual-ppp** *number*
Parameter Description	*number*: Indicates the ID of a specified virtual-ppp interface.
Command Mode	Global configuration mode
Usage Guide	N/A

Setting Pseudowire Rules

Command	**pseudowire** *peer-ip-address vcid* { **encapsulation l2tpv2** [**pw-class** *pw-class-name*] | **pw-class** *pw-class-name* }
Parameter Description	*peer-ip-address*: Indicates the address of the remote LNS. *vcid*: Indicates the global ID. *pw-class-name*: Indicates the name of the referenced pseudowire-class interface.
Command Mode	config-if mode
Usage Guide	N/A

Configuration Example

Configuring Cisco 2620 as L2TP Server and FS Router as L2TP Client to Initiate Connection

Scenario Figure 8-3	
Configuration Steps	● Configure Cisco 2620 as an L2TP server and accept the L2TP client access. ● Configure the PAP authentication mode on the server and set both username and password to **rgnos**. ● Configure an address pool for the server so that an IP address is dynamically assigned to the tunnel after the client connected to the tunnel passes authentication. ● Configure FS router as an L2TP client. ● Configure the L2TP data transmission and encapsulation mode for the client. ● Configure a tunnel interface for the client, set pseudowire rules, and specify an address for the connected server. ● Configure the PAP authentication mode for the client and set both username and password to **rgnos**. ● Configure the negotiation mode for the client tunnel address so that an address is dynamically assigned to the client after the client passes authentication on the server. ● Enable the route between the internal network of the branch where the client is deployed and the internal network of the headquarters where the server is deployed to pass through the virtual-ppp interface.
Router	FS # configure terminal FS (config)# l2tp-class 1 FS (config)# pseudowire-class 1 FS (config-pw-class)# encapsulation l2tpv2 FS (config)# interface Virtual-ppp 1 FS (config-if-virtual-ppp 1)# pseudowire hostname mm.hxs.meibu.com 1 encapsulation l2tpv2 FS (config-if-virtual-ppp 1)# ppp pap sent-username rgnos password rgnos FS (config-if-virtual-ppp 1)# ip address negotiate FS (config)# ip route 192.168.19.0 255.255.255.0 Virtual-ppp 1
Verification	L2TP configuration is not required for a PC in the internal network of the branch. Network administrators need to assign an internal network address to the PC (192.168.201.213 herein) and set the gateway to 192.168.201.1. Check that the PC in the internal network of the branch successfully accesses the internal network segment 192.168.19.0 of the headquarters where

	the server is deployed.

8.4.3 Configuring L2TP Tunnel Initiated by Remote Client

Configuration Effect

- Enable the remote client to initiate an L2TP tunnel. In this case, the router accepts a connection request from the L2TP client and negotiates to establish a tunnel.

Notes

- The VPDN function of FS products is enabled/disabled immediately after configuration. If the VPDN function is disabled, all existing L2TP tunnels and sessions will be released.

Configuration Steps

Creating/Configuring Local Address Pool

- Optional.
- If an IP address to be used in a VPN is not set for the remote client, an IP address needs to be assigned to the remote client so that the router, serving as a PNS, accepts L2TP connections initiated by the remote client. In general, an idle IP address in a specified address pool is assigned to the client. FS products provide a command for configuring a local address pool.

Configuring User Information

- Optional.
- User information is used to conduct user identity authentication on clients that attempt to remotely access the local device via L2TP. The router locally maintains a database that stores names and passwords of users who are allowed to access (dial in to) the local device.

Enabling VPDN Congestion Control

- Optional.
- This option is mandatory if VPDN congestion control needs to be enabled.

Enabling VPDN Function

- Mandatory.
- If a router is required to accept the L2TP access from the remote client and establish an L2TP tunnel and session, the VPDN function must be enabled on the router.

Setting VPDN Source Address

- Optional.
- After the VPDN source address is set, the tunnel destination address configured for the remote client must be consistent with the VPDN source address so that an L2TP tunnel is successfully established. By default, the system does not check whether the destination address in the received tunnel establishment request is a specific value.

Setting Maximum VPDN Session Number

- Optional.
- After the maximum VPDN session number is set, an access request will be rejected if the number of existing VPDN sessions reaches the maximum value. By default, the maximum session number is the maximum value configured by this command.

Ignoring Check on Source Addresses of Packets from Peer Device

- Optional.
- This function is used to ignore errors occurring in L2TP control packets that are from the peer device and do not comply with the RFC specifications, to ensure normal negotiation. By default, the system strictly checks the source addresses of packets.

Enabling the Rate Limit Function

- Optional.
- Limit the establishment rate of VPDN tunnels so as to limit the number of VPDN tunnels that can be established at a time. By default, the rate limit function is disabled.

Creating/Configuring Specified Virtual-Template Interface

- Mandatory.
- The created virtual-template interface will be used as a configuration template of the virtual-access interface for binding and bearing L2TP sessions.

Creating/Configuring Specified VPDN-Group Unit

- Mandatory.
- The created VPDN-group unit allows a client to access and establish a tunnel.

Accepting Remote Client Dial-in

- Mandatory.
- If the local router needs to provide the PNS function, the dial-in from the remote client must be accepted.

Setting Tunnel Protocol

- Mandatory.
- The tunnel mode must be set prior to the tunnel protocol. If the local router is required to provide the PNS function, protocol pptp or protocol any must be configured.

Setting Virtual Template

- Mandatory.
- Before a virtual template is set for a VPDN-group, the tunnel mode must be set.

Setting Peer Hostname

- Optional.

- If the peer name is set, the VPDN-group is effective only to the remote client that matches the hostname. If no peer name is set, the VPDN-group becomes the default VPDN-group of the system and can provide the VPDN service for any remote client. If no peer name is set for multiple configured VPDN-groups, the system uses the first VPDN-group that meets conditions to accept the dial-in from the remote client.

Setting Local Name

- Mandatory.
- Set the local name. The local name will be used as a recording attribute and sent to the peer device. By default, FS products use the router name as the local name and send it to the peer host of a tunnel.

Setting VPDN-Group Source Address

- Mandatory.
- The destination address in the tunnel establishment request sent from the remote client must match the VPDN-group source address so that the VPDN-group is applied.

Enabling Tunnel Authentication

- Optional.
- Set an L2TP control connection parameter. By default, the establishment of L2TP tunnels does not require tunnel authentication. Tunnel authentication is required by Cisco devices by default.

Setting Transmission Interval of Hello Messages

- Optional.
- Set an L2TP control connection parameter. The default transmission interval of Hello control messages is 60 seconds.

Setting Tunnel Password

- Mandatory.
- Set an L2TP control connection parameter.

Setting Size of Receive Window for Tunnel Control Connections

- Optional.
- Set an L2TP control connection parameter. The default size of the receive window for control messages is 4.

Setting Retransmission Parameters for Tunnel Control Messages

- Optional.
- Set an L2TP control connection parameter. The default number of retransmission times of control messages is 5; the default minimum retransmission interval of control messages is 1 second, and the default maximum retransmission interval of control messages is 8 seconds.

Setting Maximum Interval for Establishing Session Connection or Control Connection of Tunnel

- Optional.

- Set an L2TP control connection parameter. The default maximum interval for establishing a session connection of a tunnel is 600 seconds, and the maximum interval for establishing a control connection of a tunnel is 300 seconds.

Enabling Packet Encryption Check (Only Encrypted Packets can Pass Through VPDN Tunnels After Command Configuration)

- Mandatory.
- Set an L2TP control connection parameter.

Supporting RFC2661-Compliant AVP Hidden Parsing Algorithm

- Mandatory.
- Set an L2TP control connection parameter.

Setting UDP Checksum to Non-null Value

- Optional.
- Set an IP/UDP parameter for L2TP message transmission. By default, on FS products, the UDP checksum field in the L2TP messages borne by L2TP tunnels is null.

Setting IP ToS Field

- Optional.
- Set an IP/UDP parameter for L2TP message transmission. By default, the ToS field in IP headers in L2TP messages is set to 0.

Setting IP Precedence Field

- Optional.
- Set an IP/UDP parameter for L2TP message transmission. By default, the precedence field in the IP headers is set to 0.

Forcibly Conducting PPP Authentication

- Mandatory.
- When the client triggers the LAC to start dialup, the LAC represents the LNS to authenticate the client. This command is used to re-authenticate the client after an L2TP tunnel is established. This command is effective only on the LNS.

Ignoring Errors Occurring in Packets from Peer Device

- Optional.
- Ignore errors occurring in L2TP control packets that are from the peer device and do not comply with the RFC specifications, to ensure normal negotiation.

Verification

- Enable the remote client to initiate an L2TP tunnel. The router accepts a connection request from the remote L2TP client, and negotiates to establish a tunnel.

Related Commands

Creating/Configuring Local Address Pool

Command	**ip local pool** *poolname first-ip [last-ip]*
Parameter Description	*poolname*: Indicates the name of the created/configured local address pool. *first-ip*: Indicates the first address in the range of the local address pool. *last-ip*: Indicates the last address in the range of the local address pool.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring User Information

Command	**username** *user-name* **password** *password*
Parameter Description	*user-name*: Indicates the name of the user who is allowed to dial in. *password*: Indicates the user password.
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling VPDN Function

Command	**vpdn enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Setting VPDN Source Address

Command	**vpdn source-ip** *ip-address*
Parameter Description	*Ip-address*: Indicates the VPDN source address.
Command Mode	Global configuration mode
Usage Guide	N/A

Setting Maximum VPDN Session Number

Command	**vpdn session-limit** *sessions*
Parameter Description	*sessions*: Indicates the maximum VPDN session number.
Command Mode	Global configuration mode
Usage Guide	N/A

Ignoring Check on Source Addresses of Packets from Peer Device

Command	**vpdn ignore_source**
Parameter Description	N/A
Command Mode	config-vpdn mode
Usage Guide	N/A

Enabling Rate Limit Function

Command	**vpdn limit_rate** *rate_num*
Parameter Description	*rate_num*: Indicates the number of tunnels that can be established per second. The value ranges from 5 to 100.
Command Mode	Global configuration mode
Usage Guide	N/A

Creating/Configuring Specified Virtual-Template Interface

Command	**interface virtual-template** *number*
Parameter Description	*number*: Indicates the serial number of a specified virtual-template interface.
Command Mode	Global configuration mode
Usage Guide	N/A

Creating/Configuring Specified VPDN-Group Unit

Command	**vpdn-group** *name*
Parameter Description	*name*: Indicates the name of a VPDN-group.
Command Mode	Global configuration mode
Usage Guide	N/A

Accepting Remote Client Dial-in

Command	**accept-dialin**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Setting Tunnel Protocol

Command	**protocol** { **any** | **l2tp** | **pptp** }
Parameter	N/A

Description	
Command Mode	config-vpdn-acc-in mode
Usage Guide	The tunnel mode must be set prior to the tunnel protocol. If the local router is required to provide the PNS function, **protocol l2tp** or **protocol any** must be configured.

Setting Virtual Template

Command	**virtual-template** *number*
Parameter Description	*number*: Indicates the serial number of a specified virtual-template interface.
Command Mode	config-vpdn-acc-in mode
Usage Guide	N/A

Setting Peer Hostname

Command	**terminate-from hostname** *name*
Parameter Description	*name*: Indicates the peer hostname.
Command Mode	config-vpdn mode
Usage Guide	N/A

Setting Local Name

Command	**local name** *name*
Parameter Description	*name*: Indicates the local name.
Command Mode	config-vpdn mode
Usage Guide	N/A

Setting VPDN-Group Source Address

Command	**source-ip** *src-ip*
Parameter Description	*src-ip*: Indicates the VPDN-group source address.
Command Mode	config-vpdn mode
Usage Guide	N/A

Enabling Tunnel Authentication

Command	**l2tp tunnel authentication**
Parameter Description	N/A

Command Mode	config-vpdn mode
Usage Guide	N/A

Setting Transmission Interval of Hello Messages

Command	**l2tp tunnel hello** *interval*
Parameter Description	*Interval*: Indicates the transmission interval of Hello messages (unit: seconds).
Command Mode	config-vpdn mode
Usage Guide	N/A

Setting Tunnel Password

Command	**l2tp tunnel password** *pass-word*
Parameter Description	*pass-word*: Indicates the tunnel password.
Command Mode	config-vpdn mode
Usage Guide	N/A

Setting Size of Receive Window for Tunnel Control Connections

Command	**l2tp tunnel receive-window** *size*
Parameter Description	*size*: Indicates the size of the receive window for tunnel control connections.
Command Mode	config-vpdn mode
Usage Guide	N/A

Setting Retransmission Parameters for Tunnel Control Messages

Command	**l2tp tunnel retransmit** { **retries** *number* | **timeout** { **min** | **max** } *seconds* }
Parameter Description	*number*: Indicates the number of retransmission times. *seconds:* Indicates the timeout time. The unit is seconds.
Command Mode	config-vpdn mode
Usage Guide	N/A

Setting Maximum Interval for Establishing Session Connection or Control Connection of Tunnel

Command	**l2tp tunnel timeout** { **no-session** | **setup**} *seconds*
Parameter Description	*seconds*: Indicates the interval (unit: seconds).
Command Mode	config-vpdn mode

Usage Guide	N/A

Enabling Packet Encryption Check (Only Encrypted Packets can Pass Through VPDN Tunnels After Command Configuration)

Command	**l2tp tunnel force_ipsec**
Parameter Description	*N/A*
Command Mode	config-vpdn mode
Usage Guide	N/A

Supporting RFC2661-Compliant AVP Hidden Parsing Algorithm

Command	**l2tp tunnel avp-hidden-compatible**
Parameter Description	N/A
Command Mode	config-vpdn mode
Usage Guide	N/A

Setting UDP Checksum to Non-null Value

Command	**l2tp ip udp checksum**
Parameter Description	N/A
Command Mode	config-vpdn mode
Usage Guide	N/A

Setting IP ToS Field

Command	**ip tos** *tos-value*
Parameter Description	*tos-value*: Indicates the value of the ToS field in IP headers in L2TP messages.
Command Mode	config-vpdn mode
Usage Guide	N/A

Setting IP Precedence Field

Command	**ip precedence** *value*
Parameter Description	*Value*: Indicates the value of the precedence field in IP headers.
Command Mode	config-vpdn mode
Usage Guide	N/A

Forcibly Conducting PPP Authentication

Command	**force-local-chap**
Parameter Description	N/A
Command Mode	config-vpdn mode
Usage Guide	N/A

Forcibly Conducting LCP Authentication

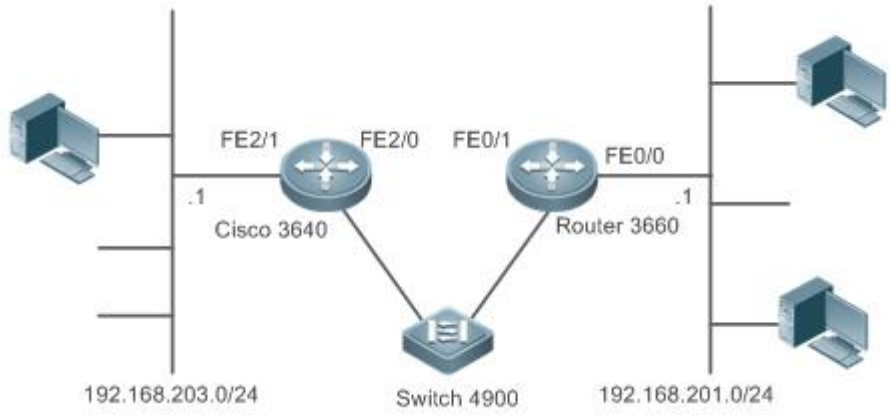
Command	**force-local-lcp**
Parameter Description	N/A
Command Mode	config-vpdn mode
Usage Guide	N/A

Ignoring Errors Occurring in Packets from Peer Device

Command	**lcp renegotiation always**
Parameter Description	N/A
Command Mode	config-vpdn mode
Usage Guide	N/A

Configuration Example

Establishing Tunnel with Cisco 3640

Scenario Figure 8-4	
Configuration Steps	● Configure the FS router as an L2TP server to provide the L2TP dial-in service. Enable the VPDN service. ● Configure a VPDN-group unit on the server, accept the dial-in from the remote client, and set the tunnel protocol to L2TP. ● Configure a local address pool on the server to assign virtual IP addresses to dial-in clients. ● On the server, set the username and password for client authentication to **user** and **pass**

	respectively. ● Configure a virtual template on the server, set the PPP authentication mode, and associate the virtual template with the local address pool. ● Configure Cisco 3640 as an L2TP client and conduct L2TP dialup by using the username and password.
Router	FS # configure terminal FS (config)# vpdn enable FS (config)# vpdn-group pptp FS (config-vpdn)# accept-dialin FS (config-vpdn)# protocol l2tp FS (config-vpdn)# virtual-template 1 FS (config)# ip local pool l2tp 1.1.1.2 1.1.1.254 FS (config)# username user password 0 pass FS (config)# interface Virtual-Template 1 FS (config-if-virtual-template-1)# ppp authentication pap FS (config-if-virtual-template-1)# ip unnumbered FastEthernet 0/1 FS (config-if-virtual-template-1)# peer default ip address pool l2tp
Verification	Configure Cisco 3640 as an L2TP client, set the VPDN server type to L2TP, set PAP authentication, and set the username and password to **user** and **pass** respectively. After the configuration is completed, perform L2TP dial-in. PCs in the internal network segment 192.168.203.0 of the L2TP client can access the server in the internal network of the L2TP server, for example, the server with the IP address of 192.168.201.79.

8.5 Monitoring

Clearing

N/A

Displaying

Description	Command
Displays information about the current VPDN tunnel and session. Displays information about the tunnel of a specified ID.	**show vpdn** [**session** | **tunnel** [**l2tp** *locid*]]
Displays online and offline information of all users or a specified user in log files.	**show vpdn log** [**user** *username*]
Displays detailed configuration of all L2TP-class interfaces or a specified L2TP-class interface configured in the system.	**show l2tp-class** [*l2tp-class-name*]

Displays detailed configuration of all pseudowire-class interfaces or a specified pseudowire-class interface configured in the system.	**show pseudowire-class** [*pseudowire-class-name*]
Clears specified tunnels.	**clear vpdn tunnel** [{ **l2tp** | **pptp** } [**id** *locid*] | [*remote-host-name*]]
Clears users' online and offline information in the log.	**clear vpdn log**

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Enables the VPDN error debugging switch.	**debug vpdn error**
Disables the VPDN error debugging switch.	**no debug vpdn error**
Enables the VPDN event debugging switch.	**debug vpdn event**
Disables the VPDN event debugging switch.	**no debug vpdn event**
Enables the VPDN packet debugging switch.	**debug vpdn packet**
Disables the VPDN packet debugging switch.	**no debug vpdn packet**
Enables the VPDN l2x-data debugging switch.	**debug vpdn l2x-data**
Disables the VPDN l2x-data debugging function.	**no debug vpdn l2x-data**
Enables the VPDN l2x-errors debugging switch.	**debug vpdn l2x-errors**
Disables the VPDN l2x-errors debugging switch.	**no debug vpdn l2x-errors**
Enables the VPDN l2x-events debugging switch.	**debug vpdn l2x-events**
Disables the VPDN l2x-events debugging switch.	**no debug vpdn l2x-events**
Enables the VPDN l2x-packets debugging switch.	**debug vpdn l2x-packets**
Disables the VPDN l2x-packets debugging switch.	**no debug vpdn l2x-packets**

9 Configuring IPSec

9.1 Overview

IP Security (IPSec) is a Layer-3 tunnel encryption protocol formulated by the Internet Engineering Task Force (IETF). It provides high-quality, interoperable, and cryptology-based security guarantee for data transmitted in the Internet. IPSec provides the following security services for specific communication parities at the IP layer via encryption and data authentication:

- Confidentiality: The IPSec sender encrypts packets prior to packet transmission in a network.
- Data integrity: The IPSec receiver authenticates data packets from the sender, to ensure that data is not tampered during transmission.
- Data authentication: The IPSec receiver authenticates whether the sender that sends IPSec packets is valid.
- Anti-replay: The IPSec receiver detects and rejects expired or repetitive packets.

The Internet Key Exchange (IKE) protocol can be configured to provide IPSec with services of automatically negotiating exchange keys and establishing and maintaining Security Associations (SAs), so as to simplify the IPSec application and management. IKE negotiation is not mandatory. The policies and algorithms used by IPSec can be manually configured.

IPSec Implementation

IPSec implements security services via the following protocols:

- Authentication Header (AH): This protocol is numbered 51, and mainly provides data authentication, data integrity check, and anti-replay functions. It supports Message Digest 5 (MD5), Secure Hash Algorithm 1 (SHA-1), and so on. An AH packet header is placed behind the standard IP header, to ensure the integrity and authenticity of data packets, and prevent hackers from intercepting data packets or inserting forged data packets to a network.
- Encapsulating Security Payload (ESP): This protocol is numbered 50. Different from AH, ESP encrypts user data to be protected and then encapsulates the data into the IP packets to ensure the data confidentiality. The encryption algorithms supported by ESP include the Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES), and so on. Moreover, the MD5 and SHA-1 algorithms are optional and can be selected to ensure the packet integrity and authenticity, which is optional.

AH and ESP can be used separately or jointly. When the device uses AH and ESP jointly, the device conducts ESP encapsulation on a packet and then conducts AH encapsulation. The encapsulated packet is composed of the original IP packet, ESP header, AH header, and external IP header from inside out.

Protocols and Standards

FS products conform to the following RFC standards:

- 2401 Security Architecture for the Internet Protocol. S. Kent, R. Atkinson. November 1998. (Format: TXT=168162 bytes) (Obsoletes RFC1825) (Obsoleted by RFC4301) (Updated by RFC3168) (Status: PROPOSED STANDARD)

- 2402 IP Authentication Header. S. Kent, R. Atkinson. November 1998. (Format: TXT=52831 bytes) (Obsoletes RFC1826) (Obsoleted by RFC4302, RFC4305) (Status: PROPOSED STANDARD)
- 2403 The Use of HMAC-MD5-96 within ESP and AH. C. Madson, R. Glenn. November 1998. (Format: TXT=13578 bytes) (Status: PROPOSED STANDARD)
- 2404 The Use of HMAC-SHA-1-96 within ESP and AH. C. Madson, R. Glenn. November 1998. (Format: TXT=13089 bytes) (Status: PROPOSED STANDARD)
- 2405 The ESP DES-CBC Cipher Algorithm With Explicit IV. C. Madson, N. Doraswamy. November 1998. (Format: TXT=20208 bytes) (Status: PROPOSED STANDARD)
- 2406 IP Encapsulating Security Payload (ESP). S. Kent, R. Atkinson. November 1998. (Format: TXT=54202 bytes) (Obsoletes RFC1827) (Obsoleted by RFC4303, RFC4305) (Status: PROPOSED STANDARD)
- 3948 UDP Encapsulation of IPsec ESP Packets. A. Huttunen, B. Swander, V. Volpe, L. DiBurro, M. Stenberg. January 2005. (Format: TXT=30366bytes) (Status: PROPOSED STANDARD)

9.2 Applications

Application	Description
Interconnecting Private Networks in Different Locations over IPSec VPN	A tunnel is established over IPSec VPN to connect LANs in different locations. Dynamic routing is not supported and networks can be established only in static routing mode.
Connecting to Private Network Through L2TP over IPSec	A tunnel is established using L2TP over IPSec to connect to a remote LAN. It is applicable to the access of small-sized networks using dynamic IP addresses.

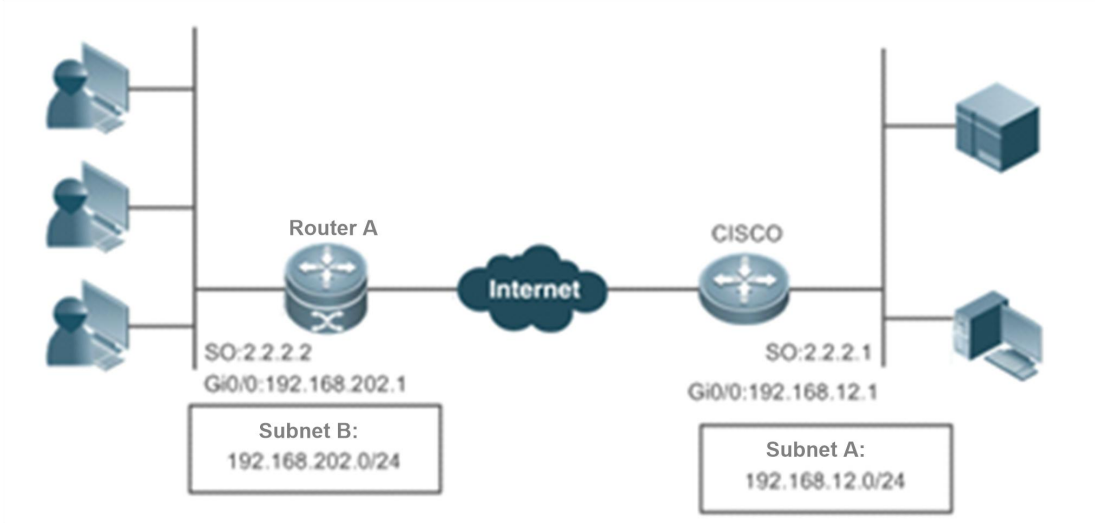
9.2.1 Interconnecting Private Networks in Different Locations over IPSec VPN

Scenario

Subnet A and Subnet B mutually access each other via an IPSec Virtual Private Network (VPN) tunnel.

- Router A is connected to a Cisco device via the Wide Area Network (WAN) and their IP addresses are reachable.
- Subnet B accesses Subnet A through the tunnel and WAN.
- Subnet A accesses Subnet B through the tunnel and WAN.

Figure 9-1



Remarks	Router A is a gateway deployed in the public network. The Cisco device is a VPN gateway deployed in the public network.

Deployment

- Connect to the WAN over the Asymmetric Digital Subscriber Line (ADSL) or in other modes.
- Implement the internal network routing and interconnection via the IPSec VPN tunnel.

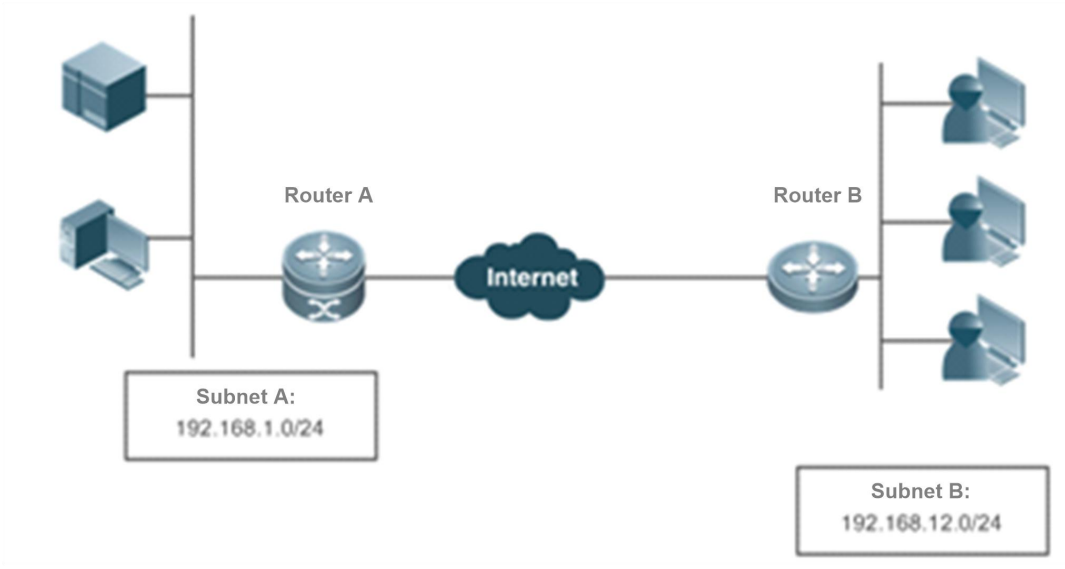
9.2.2 Connecting to Private Network Through L2TP over IPSec

Scenario

A remote private network connects to the Internet in ADSL dialup mode. IP addresses are dynamically allocated. A VPN is established to connect to the private network.

The effect of the Layer 2 Tunneling Protocol (L2TP) over IPSec is similar to that of IPSec VPN deployed separately. An L2TP over IPSec tunnel is established, which is not restricted by multicast and broadcast addresses of IPSec tunnels or interested flows. Addresses can be allocated via DHCP and a network is established in dynamic routing mode, thereby implementing reachable bidirectional route.

Figure 9-2



Remarks	Router A is a gateway deployed in the public network. Router B is a VPN gateway that connects to the Internet via dynamic addresses.

Deployment

- Establish an IPSec tunnel between Router B and Router A, to protect L2TP data destined for UDP Port 1701.
- Connect Router B to the private network via the Virtual Private Dial-up Network (VPDN).
- Assign addresses via the Authentication, Authorization, and Accounting (AAA) and add routes.
- Assign subnet addresses over the Dynamic Host Configuration Protocol (DHCP).
- Establish a route between Router A and Router B in dynamic routing mode.

9.3 Features

Basic Concepts

Security Association (SA)

IPSec provides secure communication between two end points. The end points are called IPSec peers.

SAs are the basis and essence of IPSec. An SA specifies elements agreed between communication peers. For example, an SA specifies the protocol to be used (AH, ESP, or both), protocol encapsulation mode (transport mode or tunnel mode), encryption algorithm (DES, 3DES, or AES), shared key of protected data in specific flows, and key lifetime.

An SA is unidirectional. In the bidirectional communication between two peers, at least two SAs are required to protect data flows in both directions. In addition, if both peers need to use both AH and ESP to ensure secure communication, each peer establishes an independent SA for each protocol.

An SA is uniquely identified by a triplet. The triplet includes the Security Parameter Index (SPI), destination IP address, and security protocol ID (AH or ESP).

SPI is a 32-bit value generated for uniquely identifying an SA. It is placed in the AH header and ESP header for transmission. When an SA is manually configured, you need to manually specify the SPI. When an SA is established by means of IKE negotiation, SPI is randomly generated.

An SA has a lifetime and only SAs that are established via IKE negotiation have lifetime. SAs are classified into two types:

- Time-based SAs. A time-based SA defines the duration from establishment to the expiration of an SA.
- Traffic-based SAs. A traffic-based SA defines the maximum traffic that can be processed by an SA.

When the lifetime of an SA reaches the specified time or traffic, the SA will expire. Before an SA expires, IKE negotiates and establishes a new SA for IPSec. In this way, a new SA is available before the old SA expires. The old SA is still used to protect communication before a new SA is agreed on. After the new SA is agreed on, the new SA will be immediately used to protect communication.

Encapsulation Mode

IPSec supports two work modes:

- Tunnel mode: In this mode, an entire IP packet is used to calculate the AH header or ESP header. The AH header or ESP header and user data encrypted using ESP are encapsulated into a new IP data packet. The tunnel mode is usually applied to the communication between two security gateways.
- Transport mode: In this mode, only transport-layer data is used to calculate the AH header or ESP header. The AH or ESP header and user data encrypted using ESP are placed behind the original IP header. The transport mode is usually applied to the communication between two hosts, or between one host and one security gateway. It cannot be used to protect forwarded data.

Authentication Algorithm and Encryption Algorithm

(1) Authentication algorithm

The authentication algorithm is implemented using the hash function. The hash function is an algorithm that allows input of messages of any length and generates output of a fixed length. The output is called message digest. Both IPSec peers calculate the message digests. If two message digests are the same, it indicates that packets are complete and are not tampered. IPSec uses two authentication algorithms:

- MD5: Generates a 128-bit message digest via the input message of any length.
- SHA-1: Generates a 160-bit message digest via the input message of less than 264 bits.

The MD5 algorithm is faster than the SHA-1 algorithm in calculation speed but poorer in security strength.

(2) Encryption algorithm

The encryption algorithm is implemented using the symmetric key system. It uses the same key to encrypt and decrypt data. IPSec supports three encryption algorithms:

- DES: Uses a 56-bit key to encrypt a 64-bit plaintext block.
- 3DES: Use three 56-bit DES keys (totaling 168 bits) to encrypt the plaintext.
- AES: Uses a key of 128 bits, 192 bits, or 256 bits to encrypt the plaintext.

The security ranking of the three encryption algorithms is AES, 3DES, DES in descending order. The implementation mechanism of an encryption algorithm with high security is complex and the operation speed is slow. The DES algorithm can meet common security requirements.

Negotiation Mode

SAs can be established in two negotiation modes:

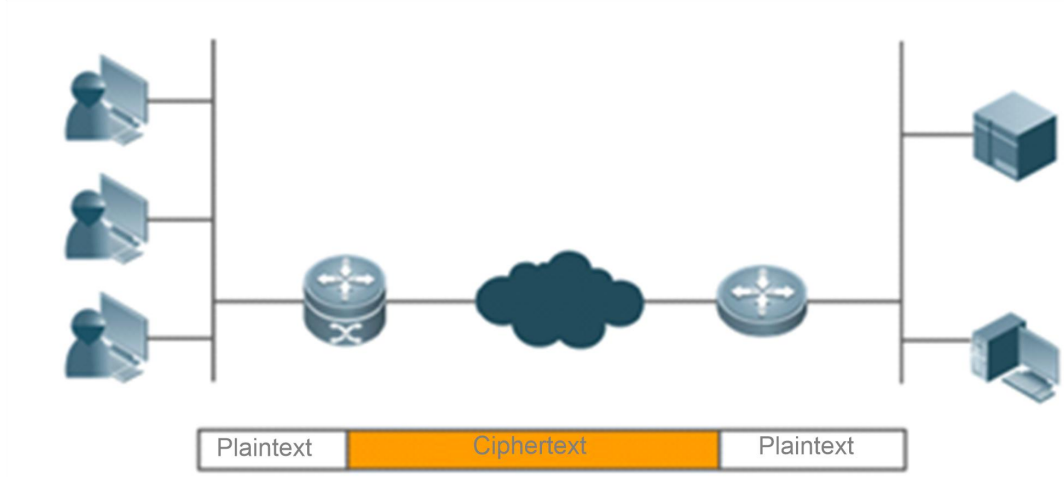
- The manual mode is complex. All information required for creating an SA must be manually configured, and the manual mode does not support some advanced features (such as periodical key update). Nevertheless, this mode can implement the IPSec function separately without relying on the IKE.
- The IKE automatic negotiation mode, in which the Internet Security Association and Key Management Protocol (ISAKMP) is used, is relatively simple. After an IKE negotiation security policy is configured, IKE automatically negotiates to establish and maintain SAs.

When a few peers communicate with the device or in a small-sized static environment, SAs can be manually configured. For large- and medium-sized dynamic network environments, IKE negotiation is recommended for establishing SAs.

Security Tunnel

A security channel is an interconnection channel established between the local end and the peer end. It consists of one or more SA pairs.

Figure 9-3 shows an example of IPSec protection implemented between subnets.



Requirement for the IPSec model: Interested flows are matched by priority during detection. IPSec cannot process the conflict occurring in interested flows.

Overview

Feature	Description	
IPSec Tunnel	Configuring Default Lifetime	Ensures the key security. The tunnel key needs to be updated periodically and the update interval can be changed by configuring the lifetime.
	Configuring DF Bit Coverage Function for IPSec Tunnel	Controls the DF bit after tunnel encapsulation.
	Creating Encryption Access List	Encapsulates interested flows in the tunnel. Only data in the interested flows is encapsulated.

	Defining Transformation Set	Defines the encapsulation format and relevant algorithms.
	Creating Encryption Mapping Entries	Defines a tunnel feature set.
	Configuring Multicast Policy	Configures a multicast policy. According to the RFC protocols, tunnels do not support multicast packets. Some devices, however, do not filter out multicast packets. Therefore, adjust the encapsulation logic as required to achieve compatibility.

9.3.1 IPSec Tunnel

Working Principle

You can create common manual tunnels by configuring some static policies on the CLI.

In the establishment of a tunnel using ISAKMP auto-negotiation, an encryption tunnel is established using IKE (described in the chapters below) and then an IPSec tunnel is negotiated using the IKE tunnel. The IKE tunnel is independent of the IPSec tunnel, and they are not directly associated. After the IKE tunnel is deleted, the IPSec tunnel can still exist. After the IPSec tunnel is deleted, the IKE tunnel can still exist. Therefore, IPSec tunnel-relevant control is effective only to IPSec tunnels.

Related Configuration

➘ Configuring Default Lifetime

This configuration is optional. You can use this command to change the default lifetime of the system. IKE uses this lifetime for negotiation unless otherwise specified, to ensure that the IPSec lifetime does not exceed the default lifetime.

The default lifetime of the system is 1 hour (3,600 seconds) or 4,608,000 KB of communication amount (that is, the communication lasts 1 hour at the rate of 10 MB per second). You can skip this step if you allow the default value. The default lifetime is used if no special description is provided in encryption mapping entries. When negotiating the IPSec lifetime, IKE uses the smaller value of the lifetime on the local peer and remote peer. When the lifetime of an IPSec SA expires, the IKE re-negotiates the IPSec SA and uses new parameters and keys for the IPSec SA so that the IPSec SA functions properly.

An SA and relevant keys time out upon the expiration of the lifetime that expires first. The lifetime is specified using the number of seconds (specified by the **seconds** keyword) or transmission communication amount in KBs (specified by the **kilobytes** keyword).SAs that are manually established (using the encryption mapping entry marked with **ipsec-manual**) have no lifetime limitations.

To ensure that a new SA is ready for use when the old SA expires, the new SA must be negotiated prior to the timeout of the old SA. A new SA is negotiated 30 seconds before the lifetime of the old SA expires or when the communication amount of the channel is 256 bytes apart from the lifetime (depending on the communication peer of which the SA lifetime expires first).

If no communication data passes through a channel during the lifetime of the SA, the SA will be released and no new SA will be negotiated when the lifetime expires. A new SA will be negotiated only when a packet needs to be protected by IPSec for transmission.

The default lifetime configuration of the system does not need to be changed. It needs to be changed only in special scenarios.

The lifetime can be globally configured or configured for a specific encryption mapping set.

Configuring DF Bit Coverage Function for IPSec Tunnel

Set whether fragmentation is allowed for IP packets encapsulated using IPSec.

The DF bit coverage function allows a customer to specify whether the device sets the DF bit to 0 or 1, and copies the encapsulated packer header.

The DF bit in the IP packet header determines whether the device allows fragmentation. The value **1** indicates packets cannot be fragmented and the value **0** indicates packets can be fragmented. In IPSec tunnel mode, this function enables the device to control, globally or at the interface layer, whether the DF bit in the IP header encapsulated by IPSec is determined based on the DF bit value in the original IP header. This function is supported only in tunnel mode.

The device performs the zero-out operation by default, indicating that fragmentation is allowed. This function needs to be configured in scenarios with special requirements.

This function can be configured globally only.

Creating Encryption Access List

An encryption access list is used to specify the data flows to be protected by the device. IPSec filters incoming and outgoing packets according to the encryption access list. It protects outgoing data that matches the encryption access list, and checks the validity of incoming packets that match the encryption access list.

An encryption access list is actually a common ACL, and is referenced in encryption mapping entries. An encryption access list is mandatory in static configuration mode. In dynamic mode, an encryption access list can be learnt; in profile mode, no encryption access list needs to be configured, but L2TP over IPSec is applied to encrypt L2TP tunnel packets.

The encryption access list specified in IPSec encryption mapping entries supports the four functions below:

- The encryption access entry that references the deny configuration in the ACL is not used for tunnel negotiation but used as special configuration. Data that meets the entry will not be encrypted.
- The encryption access list screens the outbound communication data to be encrypted and protected by IPSec (permit = protection). The image screening policy is automatically generated and it does not need to be configured in both directions.
- When the negotiation of an IPSec SA starts, the encryption access list specifies the data flows to be protected by the new SA.
- In the processing of inbound communication, the encryption access list is used to filter out and discard communication data that should have been protected by IPSec.
- When IKE negotiation initiated by IPSec peers is processed, the encryption access list is used to determine whether to allow the application for an IPSec SA for interested flows (negotiation is required only for IPSec ISAKMP encryption mapping entries). The ACLs at both peers must be matched. It is recommended that ACLs at both peers be the same.

IPSec filters incoming and outgoing packets according to the encryption access list. It protects outgoing data that matches the encryption access list, and checks the validity of incoming packets that match the encryption access list. Each encryption mapping set is used to protect a different interested flow on the same interface and the encryption mapping set configuration cannot conflict. Otherwise, the tunnel configured later cannot forward data.

Interested flows do not need to be configured only in dynamic mode. It is mandatory in other cases.

Defining Transformation Set

A transformation set is used to instruct a device how to protect data flows. A transformation set is a combination of specific security protocols and algorithms. It specifies the algorithm, security protocol, and data encapsulation mode. Users must specify the protection degree and requirements in a transformation set.

The following table describes all transformation sets supported by the system.

Algorithm Combination	Description
ah-md5-hmac	AH protocol and MD5 HMAC authentication algorithm
ah-sha-hmac	AH protocol and SHA HMAC authentication algorithm
esp-des	ESP protocol and DES encryption algorithm
esp-3des	ESP protocol and 3DES encryption algorithm
esp-aes-128	ESP protocol and AES encryption algorithm using a 128-bit key
esp-aes-192	ESP protocol and AES encryption algorithm using a 192-bit key
esp-aes-256	ESP protocol and AES encryption algorithm using a 256-bit key
ah-md5-hmac esp-des	AH protocol and MD5 HMAC authentication algorithm outside; ESP protocol and DES encryption algorithm inside
ah-sha-hmac esp-des	AH protocol and SHA HMAC authentication algorithm outside; ESP protocol and DES encryption algorithm inside

ah-md5-hmac esp-des esp-md5-hmac	AH protocol and MD5 HMAC authentication algorithm outside; ESP protocol, DES encryption algorithm, and MD5 HMAC authentication algorithm inside
ah-md5-hmac esp-null esp-md5-hmac	AH protocol and MD5 HMAC authentication algorithm outside; ESP protocol, zero encryption algorithm, and MD5 HMAC authentication algorithm inside
ah-md5-hmac esp-des esp-sha-hmac	AH protocol and MD5 HMAC authentication algorithm outside; ESP protocol, DES encryption algorithm, and SHA HMAC authentication algorithm inside
ah-md5-hmac esp-null esp-sha-hmac	AH protocol and MD5 HMAC authentication algorithm outside; ESP protocol, zero encryption algorithm, and SHA HMAC authentication algorithm inside
ah-sha-hmac esp-des esp-md5-hmac	AH protocol and SHA HMAC authentication algorithm outside; ESP protocol, DES encryption algorithm, and MD5 HMAC authentication algorithm inside
ah-sha-hmac esp-null esp-md5-hmac	AH protocol and SHA HMAC authentication algorithm outside; ESP protocol, zero encryption algorithm, and MD5 HMAC authentication algorithm inside
ah-sha-hmac esp-des esp-sha-hmac	AH protocol and SHA HMAC authentication algorithm outside; ESP protocol, DES encryption algorithm, and SHA HMAC authentication algorithm inside
ah-sha-hmac esp-null sp-sha-hmac	AH protocol and SHA HMAC authentication algorithm outside; ESP protocol, zero encryption algorithm, and SHA HMAC authentication algorithm inside
esp-des esp-md5-hmac	ESP protocol, DES encryption algorithm, and MD5 HMAC authentication algorithm
esp-null esp-md5-hmac	ESP protocol, zero encryption algorithm, and MD5 HMAC authentication algorithm
esp-des esp-sha-hmac	ESP protocol, DES encryption algorithm, and SHA HMAC authentication algorithm
esp-null esp-sha-hmac	ESP protocol, zero encryption algorithm, and SHA HMAC authentication algorithm
esp-3des	ESP protocol and 3DES encryption algorithm
esp-3des esp-sha	ESP protocol, 3DES encryption algorithm, and SHA HMAC authentication algorithm
esp-3des esp-md5	ESP protocol, 3DES encryption algorithm, and MD5 HMAC authentication algorithm
ah-md5-hmac esp-des	AH protocol and MD5 HMAC authentication algorithm outside; ESP protocol and 3DES encryption algorithm inside
ah-sha-hmac esp-des	AH protocol and SHA HMAC authentication algorithm outside; ESP protocol and 3DES encryption algorithm inside
ah-md5-hmac esp-3des esp-sha	AH protocol and MD5 HMAC authentication algorithm outside; ESP protocol, 3DES encryption algorithm, and SHA HMAC authentication algorithm inside
ah-sha-hmac esp-3des esp-sha	AH protocol and SHA HMAC authentication algorithm outside; ESP protocol, 3DES encryption algorithm, and SHA HMAC authentication algorithm inside

ah-md5-hmac esp-3des esp-md5	AH protocol and MD5 HMAC authentication algorithm outside; ESP protocol, 3DES encryption algorithm, and MD5 HMAC authentication algorithm inside
ah-sha-hmac esp-3des esp-md5	AH protocol and SHA HMAC authentication algorithm outside; ESP protocol, 3DES encryption algorithm, and MD5 HMAC authentication algorithm inside

In general, the esp-des combination (no data authentication) can meet the requirements. If you need to authenticate data, you can use esp-des esp-md5-hmac or esp-des esp-sha-hmac.

A transformation set is mandatory and can be referenced in multiple encryption mapping sets. Multiple transformation sets can be configured for one encryption mapping set. Transformation sets are matched by priority, and repetitive content of transformation sets does not affect negotiation results.

Creating Encryption Mapping Entry

An encryption mapping entry is used to associate the predefined ACL with transformation sets and define keys and peer addresses to form a complete IPSec solution description.

An encryption mapping set is mandatory and can be referenced by multiple interfaces.

Configuring Multicast Policy

A multicast policy is used to disable IPSec encapsulation on multicast and broadcast packets.

By default, packets are encrypted when they meet the interested flows configuration, regardless of whether they are multicast packets.

The configuration is optional.

Applying Encryption Mapping Entry to Interface

Activate a defined IPSec scheme. Apply an encryption mapping entry to an interface so that the encryption mapping set works on the interface.

Creating Profile Encryption Mapping Entry

Create a profile encryption mapping entry for establishing an SA using IKE.

Applying Profile Encryption Mapping Entry to Tunnel Interface

Apply a profile encryption mapping set to a tunnel interface.

Activate a tunnel after the configuration is applied to the tunnel interface. The tunnel does not affect data forwarding prior to tunnel activation.

An encryption mapping set can be applied only to a Layer-3 interface. It cannot be configured on Layer-2 ports such as the switching port.

9.4 Configuration

Configuration	Description and Command	
Configuring IPSec	**crypto ipsec security-association lifetime**	Configures the default lifetime.
	crypto ipsec df-bit	Configures the DF bit coverage function for the IPSec tunnel.
	access-list	Creates an encryption access list.

	crypto ipsec transform-set	Defines a transformation set.
	crypto map **crypto ipsec profile**	Creates an encryption mapping entry.
Applying IPSec	**crypto map**	Applies IPSec to an interface.

9.4.1 Configuring IPSec

Configuration Effect

- Configure IPSec tunnel negotiation function for establishing a tunnel.

Notes

- The negotiation will not be initiated if the configuration is incomplete.
- In transport mode, interested flows must be host-to-host traffic. Otherwise, the negotiation is automatically conducted in tunnel mode.
- The interested flow conflict cannot be detected. In static configuration mode, interested flows are matched by the configuration sequence; in dynamic mode, a tunnel established later has a higher priority than a tunnel established earlier.

Configuration Steps

(Optional) Configuring Default Lifetime

- This configuration is optional. You can use this command to change the default lifetime of the system. IKE uses this lifetime for negotiation unless otherwise specified, to ensure that the IPSec lifetime does not exceed the default lifetime.
- The default lifetime configuration of the system does not need to be changed. It needs to be changed only in special scenarios.
- The lifetime can be globally configured or configured for a specific encryption mapping set.

(Optional) Configuring DF Bit Coverage Function for IPSec Tunnel

- Set whether fragmentation is allowed for IP packets encapsulated using IPSec.
- The device performs the zero-out operation by default, indicating that fragmentation is allowed. This function needs to be configured in scenarios with special requirements.
- This function can be configured globally only.

Creating Encryption Access List

- An encryption access list is used to specify the data flows to be protected by the device. IPSec filters incoming and outgoing packets according to the encryption access list. It protects outgoing data that matches the encryption access list, and checks the validity of incoming packets that match the encryption access list. Each encryption mapping set is used to protect a different interested flow on the same interface and the encryption mapping set configuration cannot conflict. Otherwise, the tunnel configured later cannot forward data.
- Interested flows do not need to be configured only in dynamic mode. It is mandatory in other cases.
- When interested flow configuration references an extended ACL, it is referenced in the encryption mapping set.

Defining Transformation Set

- A transformation set is used to instruct a device how to protect data flows. A transformation set is a combination of specific security protocols and algorithms. It specifies the algorithm, security protocol, and data encapsulation mode. Users must specify the protection degree and requirements in a transformation set.
- A transformation set is mandatory and can be referenced in multiple encryption mapping sets. Multiple transformation sets can be configured for one encryption mapping set. Transformation sets are matched by priority, and repetitive content of transformation sets does not affect negotiation results.

Creating Encryption Mapping Entry

- An encryption mapping entry is used to associate the predefined ACL with transformation sets and define keys and peer addresses to form a complete IPSec solution description.
- An encryption mapping set is mandatory and can be referenced by multiple interfaces.

Verification

- Run the **show crypto map** command to display the configuration integrity. If information is displayed, it indicates that the configuration is complete.
- Run the **show crypto transform-set** command to display the configuration.
- Run the **show crypto map detail** command to display the configuration.

Related Commands

Configuring Default Lifetime

Command	**crypto ipsec security-association lifetime** { **seconds** *seconds* | **kilobytes** *kilobytes* }
Parameter Description	*seconds*: Indicates the SA timeout time (unit: seconds). The default value is **3,600** seconds (1 hour). It can be set to **0**, indicating that the time timeout function is disabled. *Kilobytes*: Indicates the SA timeout communication amount (unit: KB). The default value is **4,608,000** KB. It can be set to **0**, indicating that the byte timeout function is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring DF Bit Coverage Function for IPSec Tunnel

Command	**crypto ipsec df-bit** { **clear** | **set** | **copy** }
Parameter Description	**clear**: Zeroes out the DF bit in the external IP header. The device may fragment packets and encapsulate the data via IPSec. **set**: Sets the DF bit to 1 in the external IP header. If the DF bit in the original IP header is zeroed out, the device may fragment packets. **copy**: Uses the original DF bit value as the DF bit value of the external header. The default value is **copy**.
Command Mode	Global configuration mode
Usage Guide	N/A

Creating Encryption Access List

Command	**access-list** *access-list-number* { **deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**log**]
Parameter Description	**deny**: Ignores the target flow. **permit**: Allows the target interested flow. *protocol*: Indicates the protocol. *source source-wildcard*: Indicates the source IP address or network segment of the interested flow. *destination destination-wildcard*: Indicates the destination IP address or network segment. **log**: Enables the ACL log function.
Command Mode	Global configuration mode
Usage Guide	Describe the data flows via the source address, destination address, wildcard, communication protocol, and communication interface of the data flows. The **permit** keyword enables all IP communication that meets specified conditions to be encrypted and protected by the policy described in encryption mapping entries. The **deny** keyword exempts communication data from encryption and protection specified in specific encryption mapping entries.

Defining Transformation Set

Command	**crypto ipsec transform-set** *transform-set-name transform1 [transform2 [transform3]]*
Parameter Description	*transform-set-name*: Indicates the name of an encryption transformation set. *transform1, transform2, transform3*: Indicates the encryption mode and authentication mode.
Command Mode	Global configuration mode
Usage Guide	1. A set is a combination of security protocols, algorithms, and other settings of communication protected by IPSec. During IPSec SA negotiation, peers must use the same specific transformation set to protect specific data flows. 2. Configure multiple transformation sets and then specify one or several of them in the encryption mapping entries. Transformation sets defined in encryption mapping entries are used to negotiate IPSec SAs, so as to protect data flows that match the ACL referenced in encryption

	mapping entries. During negotiation, both peers search for the same transformation set that is available on both peers. When such a transformation set is found, it is selected as a part of IPSec SAs of both peers and applied to protected communication data. 3. If an SA is configured manually, no parameter needs to be negotiated for the SA. Therefore, the same transformation set must be specified on both peers.
Command	**mode** {**tunnel** | **transport**}
Parameter Description	**tunnel**: Indicates the tunnel mode. **transport**: Indicates the transport mode.
Command Mode	Encryption transformation set definition mode
Usage Guide	Mode setting is effective only to communication using addresses of IPSec peers as the source and destination addresses, and is ineffective to other communication (other communication is made in tunnel mode). If the communication to be protected uses the IP addresses same as the IP addresses of IPSec peers (that is, the source and destination IP addresses are both IP addresses of IPSec peers) and the transport mode is specified, the device will apply for the transport mode during negotiation and the device can allow both transport mode and tunnel mode. If the tunnel mode is specified, the device will apply for the tunnel mode and allows only the tunnel mode.

Creating Encryption Mapping Entry

Command	**crypto map** *map-name seq-num* **ipsec-isakmp** **crypto ipsec profile** *profile-name*
Parameter Description	*map-name*: Indicates the name of an encryption mapping set. *seq-num*: Indicates the priority of the encryption mapping set. *profile-name*: Specifies that there is no priority in profile mode.
Command Mode	Global configuration mode
Usage Guide	Mandatory parameters of an IPSec tunnel are configured in encryption mapping set mode. Configure the peer address, encryption transformation set, and interested flow to be referenced.

Command	**match address** *access-list-id*
Parameter Description	*access-list-id*: Indicates the ACL No. (100-199, 2000-2699, and 2900-3899). Encryption mapping uses only IP extended ACL.
Command Mode	Encryption mapping configuration mode
Usage Guide	This command specifies the ACL for an encryption mapping entry. An encryption mapping entry determines the data to be protected by IPSec according to the ACL. The ACL specified by this command is applied to both outbound and inbound communication data. If it is detected that outbound data matches the ACL and an SA is already established, the device encrypts and forwards the data. If no SA is established, the device triggers the SA negotiation (using IKE). If it is detected that inbound data matches the ACL, the device decrypts the encrypted data and directly discards data that is not encrypted.

Command	**set peer** { *hostname* | *ip-address* }
Parameter Description	*ip-address*: Indicates the IP address of the remote peer. *Hostname*: Indicate the host name of the remote peer.
Command Mode	Encryption mapping configuration mode
Usage Guide	A remote peer must be specified for an encryption mapping set in use. Multiple remote peers can be configured for an encryption mapping set. Negotiation will be initiated according to the peer configuration sequence. When the negotiation using a peer fails, the IP address of the next peer will be used for negotiation.

Command	**set transform-set** *transform-set-name1* [*transform-set-name2...transform-set-name6*]
Parameter Description	*transform-set-name*: Indicates a referenced encryption transformation set.
Command Mode	Encryption mapping configuration mode
Usage Guide	A transformation set is indispensable for successful establishment of an SA. Use this command to specify a transformation set when any encryption mapping set is configured. You can configure multiple transformation sets and select one of them for negotiation.

9.4.2 Applying IPSec

Configuration Effect

- Apply IPSec configuration to an interface so that the device automatically creates tunnel control information.

Notes

- Before IPSec is applied to an interface, all IPSec configuration does not take effect.
- IPSec tunnels can be applied only to Layer-3 interfaces.
- The same encryption mapping set can be applied to multiple interfaces, and the encryption mapping set is separately applied to multiple interfaces is independent.

Configuration Steps

Applying Encryption Mapping Entry to Interface

- Activate a defined IPSec scheme. Apply an encryption mapping entry to an interface so that the encryption mapping set works on the interface. The configuration is mandatory. Encryption mapping entries can be applied only to Layer-3 interfaces.

Verification

- Run the **show crypto ipsec sa** command to display the configuration integrity. If information is displayed, it indicates that the configuration is complete.
- Run the **show crypto map detail** command to display the configuration.

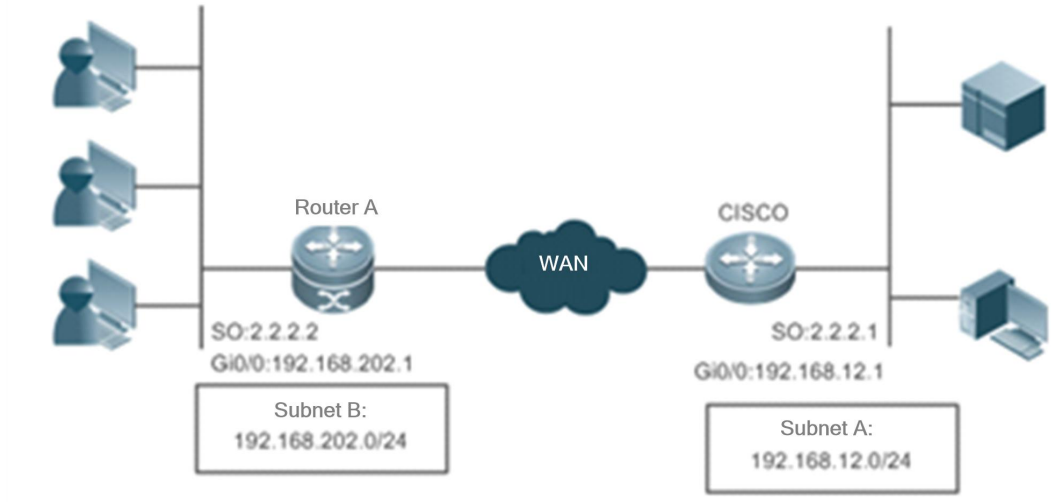
Related Commands

Applying Encryption Mapping Entry to Interface

Command	**crypto map** *map-name*
Parameter Description	*map-name*: Indicates the name of an encryption mapping set.
Command Mode	Interface configuration mode
Usage Guide	Use this command to apply an encryption mapping set to an interface. An encryption mapping set must be applied to an interface so that IPSec encryption and protection can be provided for data on the interface. One interface can be associated with only one encryption mapping set. If multiple encryption mapping entries share the same **map-name** value but different **seq-num** values, these encryption mapping entries belong to the same encryption mapping set and are applied to the same interface. The encryption mapping entry with a smaller **seq-num** value has a higher priority and is used for data matching first.

Configuration Example

Connecting Central Device to Remote Device over IPSec

Scenario Figure 9-4	
Configuration Steps	● An IPSec VPN tunnel is a point-to-point encryption tunnel. Devices at both ends of the tunnel encrypt and decrypt data via the negotiated key. IKE needs to be configured before an IPSec VPN tunnel is established. **Configuration on Router A:**
Router A	# Enable IKE. `FS(config)#crypto isakmp enable`

```
FS(config)#crypto isakmp policy 1
FS(isakmp-policy)#authentication pre-share
FS(isakmp-policy)#encrytiong 3des
```

Configure a pre-shared key and transformation set.

```
FS(config)#crypto isakmp key 0 preword address 2.2.2.1
FS(config)#crypto ipsec transform-set myset   esp-des esp-md5-hmac
```

Define an encryption mapping set.

```
FS(config)#crypto map mymap 5 ipsec-isakmp
FS(config-crypto-map)# set peer 2.2.2.1
FS(config-crypto-map)# set transform-set myset
FS(config-crypto-map)# match address 101
```

Apply the encryption mapping set to an interface.

```
FS(config)#interface GigabitEthernet 0/0
FS(config-if-GigabitEthernet 0/0)#ip address 192.168.202.1 255.255.255.0
FS(config)#interface Serial 0
FS(config-if- Serial 0)#ip address 2.2.2.2 255.255.255.0
FS(config-if- Serial 0)#encapsulation ppp
FS(config-if- Serial 0)#crypto map mymap
```

Define an encryption access list to protect the IP communication between the subnet 192.168.202.0/24 and the subnet 192.168.12.0/24.

```
FS(config)#access-list 101 permit ip 192.168.202.0 0.0.0.255 192.168.12.0 0.0.0.255
```

A tunnel can also be established in manual mode to achieve tunnel encryption. IKE negotiation is not conducted in manual mode and the key is not updated periodically, resulting in poor security and ease of use.

Define a transformation set.

```
FS(config)#crypto ipsec transform-set myset   esp-des esp-md5-hmac
```

Define an encryption mapping set.

```
FS(config)#crypto map mymap 5 ipsec-manual
FS(config-crypto-map)# set peer 2.2.2.1
FS(config-crypto-map)# set session-key inbound esp 300 cipher abcdef1234567890 authenticator abcdef1234567890abcdef1234567890
FS(config-crypto-map)# set session-key outbound esp 301 cipher abcdef1234567890 authenticator abcdef1234567890abcdef1234567890
FS(config-crypto-map)# set transform-set myset
FS(config-crypto-map)# match address 101
```

Apply the encryption mapping set to an interface.

```
FS(config)#interface GigabitEthernet 0/0
FS(config-if-GigabitEthernet 0/0)#ip address 192.168.202.1 255.255.255.0
FS(config)#interface Serial 0
FS(config-if- Serial 0)#ip address 2.2.2.2 255.255.255.0
FS(config-if- Serial 0)#encapsulation ppp
```

	FS(config-if- Serial 0)#crypto map mymap # Define an encryption access list to protect the IP communication between the subnet 192.168.202.0/24 and the subnet 192.168.12.0/24. FS(config)#access-list 101 permit ip 192.168.202.0 0.0.0.255 192.168.12.0 0.0.0.255 Monitoring and debugging Monitor and debug the SA established using IKE. Send a data packet from any host in Subnet B to Subnet A. IKE negotiation is triggered. An IPSec SA is successfully established. # Enable the IKE and IPSec debugging functions. RouterA# debug crypto ipsec IPSEC debugging is on RouterA# debug crypto isakmp ISAKMP debugging is on # The following debugging information is displayed during negotiation: Get acquire: 192.168.202.0/0.0.0.255 -> 192.168.12.0/0.0.0.255 , prot 0, port 0/0 Acquire negotiate with 2.2.2.1 (36) Beginning Quick Mode exchange, M-ID of 4445127 (36) sending packet to 2.2.2.1 (I) QM_SI1_WR1 ipsec_output:423, get item acclist 101 ipsec_output:429, match 3 (36) received packet from 2.2.2.1 (I) QM_SI1_WR1 payload format: <Hdr>,<hash> <sa> <nonce> <id> (36) processing SA payload. message ID = 4445127 (36) Creating IPSec SAs. inbound SA has spi 4445127 protocol esp, DES_CBC auth MD5 outbound SA has spi 275385850 protocol esp, DES_CBC auth MD5 lifetime of 3600 seconds, soft 3570 seconds lifetime of 4608000 kilobytes, soft 256 kilobytes ipsec_output:423, get item acclist 101 ipsec_output:429, match 3 (36) sending packet to 2.2.2.1 (I) QM_IDLE (36) Phase_2 negotiate complete!
Verification	• To check whether IKE and IPSec SAs are established, run the following commands to display relevant information:
Router A	RouterA# show crypto isakmp sa destination source state conn-id lifetime(second) 2.2.2.1 2.2.2.2 QM_IDLE 36 5013

The information above shows that an IKE SA is successfully established.

```
RouterA# show crypto ipsec sa
Interface: Serial0
Crypto map tag:mymap, local addr  2.2.2.2  //The name of the encryption mapping set is mymap and the local address 2.2.2.2 is used.
media mtu 1500
local  ident (addr/mask/prot/port): (192.168.202.0/0.0.0.255/0/0))
remote  ident (addr/mask/prot/port): (192.168.12.0/0.0.0.255/0/0))
PERMIT  //Protecting the communication between 192.168.202.0/24 and 192.168.12.0/24.
current_peer: 2.2.2.1  //The address of the remote peer is 2.2.2.1.
#pkts encaps: 3, #pkts encrypt: 3, #pkts digest 3
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
#send errors 0, #recv errors 0
//Statistics, which are sequentially the number of encapsulated packets, number of encrypted packets, number of digest packets, number of decapsulated packets, number of decrypted packets, number of verification packets, number of transmission errors, and number of receiving errors.
inbound esp sas:  //SA for processing inbound packets. The protocol is ESP.
spi:0x43D3C7 (4445127)  //The SPI is 4445127.
transform: esp-des esp-md5-hmac  //The transformation set is esp-des-md5.
in use settings={Tunnel,}  //The work mode is tunnel mode.
sa timing: remaining key lifetime (k/sec): (4607999/3578)
//The remaining lifetime prior to SA expiration is 4607999 KB/3578 seconds.
IV size: 8 bytes  //The IV vector length is 8 bytes.
Replay detection support:Y  //Anti-play processing is supported.
outbound esp sas:  //SA for processing outbound packets. The protocol is ESP.
spi:0x106A0DFA (275385850)  //The SPI is 275385850.
transform: esp-des esp-md5-hmac  //The transformation set is esp-des-md5.
in use settings={Tunnel,}  //The work mode is tunnel mode.
sa timing: remaining key lifetime (k/sec): (4607999/3577)
//The remaining lifetime prior to SA expiration is 4607999 KB/3577 seconds.
IV size: 8 bytes  //The IV vector length is 8 bytes.
Replay detection support:Y  //Anti-play processing is supported.
```

The statistics show that an IPSec tunnel is established and data packets are protected.

Monitor and debug the SA established in manual mode.

The SA manually established starts working without negotiation. The debugging information is not displayed and only statistics can be displayed.

```
RouterA# show crypto ipsec sa
Interface: Serial0
```

```
Crypto map tag:mymap, local addr    2.2.2.2    //The name of the encryption mapping set is mymap and the local address 2.2.2.2 is used.
media mtu 1500
local   ident (addr/mask/prot/port): (192.168.202.0/0.0.0.255/0/0))
remote   ident (addr/mask/prot/port): (192.168.12.0/0.0.0.255/0/0))
PERMIT                          //Protecting the communication between 192.168.202.0/24 and 192.168.12.0/24.
current_peer: 2.2.2.1                          //The address of the remote peer is 2.2.2.1.
#pkts encaps: 8, #pkts encrypt: 8, #pkts digest 8
#pkts decaps: 8, #pkts decrypt: 8, #pkts verify 8
#send errors 0, #recv errors 0
//Statistics, which are sequentially the number of encapsulated packets, number of encrypted packets, number of digest packets, number of decapsulated packets, number of decrypted packets, number of verification packets, number of transmission errors, and number of receiving errors.
inbound esp sas:                          //SA for processing inbound packets. The protocol is ESP.
spi: 0x12C (300)                                          //The SPI is 300.
transform: esp-des esp-md5-hmac               //The transformation set is esp-des-md5.
in use settings={Tunnel,}                                  //The work mode is tunnel mode.
no sa timing                                                  //There is no lifetime.
IV size: 8 bytes                                         //The IV vector length is 8 bytes.
Replay detection support:N                                //There is no anti-play processing.
outbound esp sas:                         //SA for processing outbound packets. The protocol is ESP.
spi: 0x12D (301)                                          //The SPI is 301.
transform: esp-des esp-md5-hmac               //The transformation set is esp-des-md5.
in use settings={Tunnel,}                                  //The work mode is tunnel mode.
no sa timing                                                  //There is no lifetime.
IV size: 8 bytes                                         //The IV vector length is 8 bytes.
Replay detection support:N                                //There is no anti-play processing.
The statistics show that an IPSec tunnel is established and data packets are protected.
```

9.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears the entire SA database. All active security threads will be deleted.	**clear crypto sa**
Clears the SA with a specific peer address.	**clear crypto sa peer** { *ip-address* | *peer-name* }

Clears the SA of a specific encryption mapping set.	**clear crypto sa map** *map-name*
Clears the SA with a specified <destination address, protocol, and SPI>.	**clear crypto sa spi** *destination-address* { **ah** | **esp** } *spi*

Displaying

Description	Command
Displays the transformation set configuration.	**show crypto ipsec transform-set**
Displays all or specified encryption mapping configuration.	**show crypto map** [*map-name*]
Displays the IPSec SA information.	**show crypto ipsec sa**
Displays the dynamic encryption mapping information.	**show crypto dynamic-map** [*tag map-name*]

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs IPSec events.	**debug crypto ipsec**
Debugs IPSec events.	**debug crypto engine**

10 Configuring IKE

10.1 Overview

In the IP Security (IPSec) implementation, the Internet Key Exchange (IKE) protocol can be used to establish a Security Association (SA). The IKE is established on the framework defined by the Internet Security Association and Key Management Protocol (ISAKMP). IKE provides IPSec with services of automatically negotiating exchange keys and establishing SAs, to simplify IPSec application and management, thereby greatly simplifying the IPSec configuration and maintenance.

IKE does not directly transmit keys in the network but uses a series of exchange data to calculate the key shared by both parties. Even if a third party intercepts all exchange data used for calculating a key, the third party cannot calculate the authentic key.

Functions of IKE in IPSec

- IKE enables IPSec to automatically negotiates many parameters such as the key, thereby reducing the manual configuration complexity.
- During the Diffie-Hellman (DH) exchange of IKE, each calculation is irrelevant to the generated result. The DH exchange is performed during establishment of each SA, which ensures that keys used by SAs are irrelevant.
- IPSec uses the SN in the IP packet header to implement anti-replay. The SN is a 32-bit value. After the value overflows, an SA needs to be re-established to implement anti-replay. This process needs the cooperation of IKE.
- The authentication and management of the identity of each party in secure communication will affect IPSec deployment. The large-scale application of IPSec needs the participation of the Certificate Authority (CA) or other organs that manage identity data in a centralized manner.
- IKE provides end-to-end dynamic authentication.

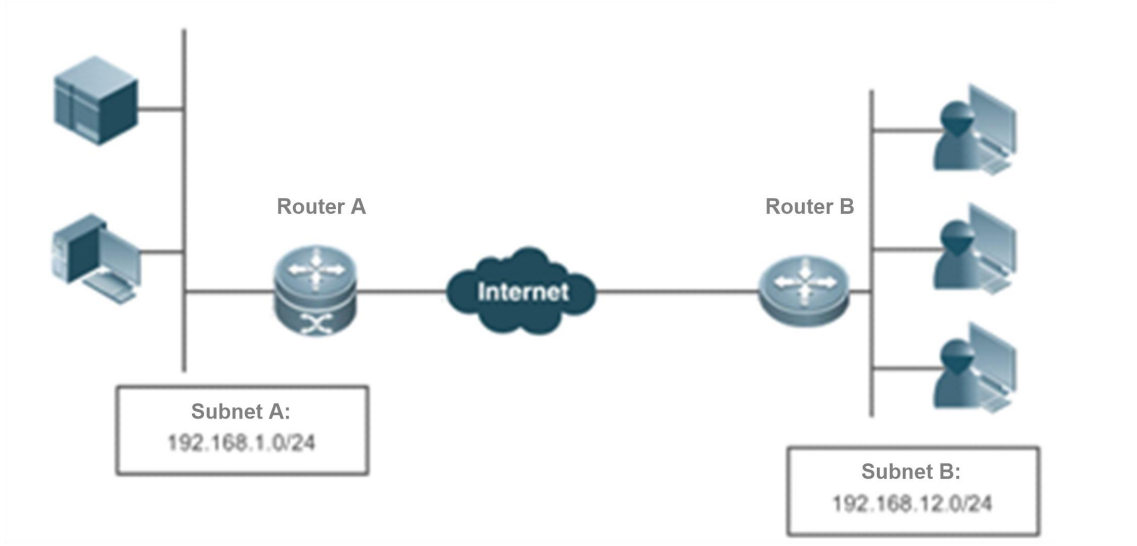
10.2 Applications

10.2.1 Establishing Dynamic VPN Tunnel

Scenario

A VPN tunnel in the star topology is established when the peer IP address is unknown on the convergence side.

Figure 10-1



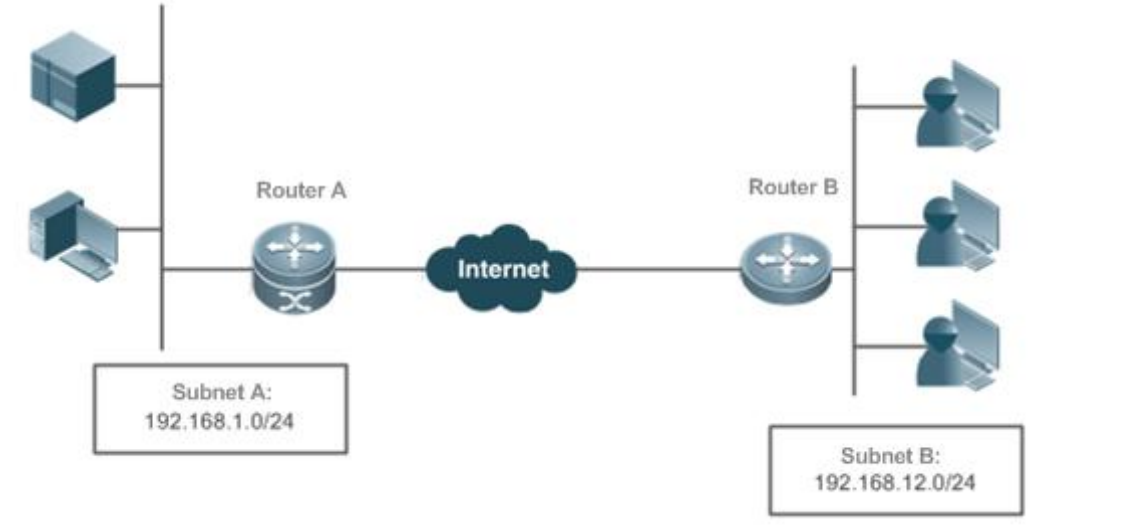
Deployment

- Connect to the WAN over the Asymmetric Digital Subscriber Line (ADSL) or in other modes.
- Establish an IKE tunnel via a public key.
- Implement the internal network routing and interconnection via the IPSec VPN tunnel.
- Establish routes via reverse routing.

10.2.2 Establishing Tunnel via Domain Name

An IKE tunnel is estalbished via a domain name when the server IP address is unknown on the access side.

Figure 10-2



Deployment

- Find out the server IP address by means of domain name resolution.
- Query the preset key by using a domain name as the authentication ID, and mutually authenticate devices to establish an IKE tunnel.
- Implement the internal network routing and interconnection via the IPSec VPN tunnel.
- Establish routes via reverse routing.

10.3 Features

IKE Security Mechanism

IKE has a self-protection mechanism, which can securely authenticate identities, distribute keys, and establish IPSec SAs on an insecure network.

1. Data authentication

Data authentication involves two aspects:

- Identity authentication: Identity authentication determines identities of both communication parties. It supports three authentication methods: pre-shared key (pre-shared-key) authentication, and PKI-based digital signature (rsa-signature) authentication.
- Identity protection: Identity data is encrypted for transmission after keys are generated, thereby implementing protection of identity data.

2. DH

Diffie-Hellman (DH) algorithm is a public key algorithm. Both communication parties exchange some data and calculate the pre-shared key when keys are not transmitted. Even if a third party (such as a hacker) intercepts all exchange data used for calculating the key, the third party cannot calculate the authentic key because of high complexity of the DH algorithm. Therefore, the DH exchange technology ensures that both parties securely obtain pubic information.

3. PFS

The Perfect Forward Secrecy (PFS) feature is a security feature, which indicates that the cracking of one key does not affect the security of other keys because these keys have no derivation relationship. IPSec is implemented using one key exchange added in the negotiation of IKE phase 2. The PFS feature is ensured using the DH algorithm.

IKE Exchange Process

IKE negotiates keys and establishes SAs for IPSec in two phases:

(1) Phase 1: Both communication parties establish a channel that passes identity authentication and security protection, that is, establish an ISAKMP SA. In Phase 1, there are two IKE exchange modes: main mode and aggressive mode.

(2) Phase 2: IKE uses the secure channel established in Phase 1 to negotiate the security service for IPSec. That is, IKE negotiates the specific SA used for secure transmission of IP data.

The IKE negotiation in main mode in Phase 1 covers three pairs of messages:

- The first pair is SA exchange messages, which are used to negotiate and determine the relevant security policy.
- The second pair is key exchange messages, which are used to exchange the Diffie-Hellman public value and auxiliary data (such as random number). The key is generated in this phase.
- The last pair is messages that carry ID information and authentication exchange data, which are used to authenticate identities and content exchanged in Phase 1. The major difference between exchange in aggressive mode and that in main mode is as follows: Identity protection is not provided and only three messages are exchanged in aggressive mode. In scenarios with low requirements for identity protection, the aggressive mode, in which a few packets are exchanged, can improve the negotiation speed. The main mode should be used in scenarios with high requirements for identity protection.

Working Principle

IKE is a key management protocol and is used in combination with IPSec. IPSec is an IP security function that provides robust authentication and IP packet encryption. IPSec can be configured without IKE. IKE, however, can provide additional functions and flexibility, and facilitate IPSec configuration, thereby enhancing functions of IPSec. IKE is a hybrid protocol, which implements the Oakley key exchange and Skeme key exchange (ISAKMP, Oakley, and Skeme are security protocols implemented by IKE) inside the Internet Security Association and Key Management Protocol (ISAKMP) framework.

IPSec (IKE-reliant IPSec) must be configured and applied to interfaces before IKE starts working. When outgoing data packets that meet requirements are detected on an interface, IPSec triggers IKE to negotiate with IKE of the remote peer. They establish a secure channel between the peers, transmit supported various IPSec parameters, and finally establish consistent SAs at both ends so that IPSec of both parties works properly. When the lifetime of IPSec SAs expires after a period of time, if data that meets requirements needs to be transmitted, the IKE modules of both peers re-negotiate IPSec again and the process repeats.

With IKE, you do not need to manually specify all IPSec parameters and keys in the encryption mapping tables of both communication parties. IKE allows specifying the lifetime of IPSec SAs, enables IPSec to periodically update keys so as to enhance the security, and enables IPSec to provide the anti-replay service.

Overview

Feature	Description	
IKE Tunnel	Enabling or Disabling IKE	Disables the IKE function during debugging.
	Ensuring Compatibility Between ACL and IKE	Checks the configuration validity.
	Creating IKE Policy	Configures an IKE negotiation policy.
	Selecting Work Mode	Selects the main mode or active mode.
	Configuring Local Identity	Configures the local identity according to the agreement of both parties. The local identity is an ID that needs to be exchanged with a negotiated object.
	Configuring Automatic Identification of Work Mode	Automatically identifies the main mode and active mode.
	Configuring Pre-shared Key	Configures a pre-shared key by IP address or host name.

	Configuring DPD Detection	Enables the DPD function and sets parameters.
	Setting IKE Negotiation Rate	Sets the IKE negotiation rate.
	Setting NAT Traversal Timeout Parameter	Sets the NAT traversal parameter.

10.3.1 IKE Tunnel

Working Principle

Configure IKE negotiation parameters used for negotiating the IKE tunnel establishment.

Related Configuration

Enabling or Disabling IKE

The IKE function is enabled by default. If you do not want to use IKE and IPSec together, you can run a command to disable the IKE function. In this case, IPSec SAs can be established only in manual mode.

The IKE function is enabled by default. It can be disabled using a command in special cases.

Ensuring Compatibility Between ACL and IKE

IKE is an application that runs over UDP. It uses UDP data packets and Port 500. If an ACL (firewall) is configured on the device to deny the UDP communication packets, the IKE negotiation will fail. Therefore, ensure that communication packets of IKE are not denied.

Creating IKE Policy

Both parties participating in IKE negotiation have at least one consistent IKE policy, which is indispensable for successful IKE negotiation. Multiple prioritized policies must be created on each pair of peers, to ensure that at least one policy matches a policy on the remote peer.

Each IKE policy defines five parameters:

Parameter	Keyword	Optional Value	Default Value
Encryption algorithm	des	56-bit DES-CBC	56-bit DES-CBC
	3des	168-bit 3DES-CBC	
	aes	128-bit AES-CBC	
Hash algorithm	sha	SHA-1 (HMAC variant)	SHA-1 (HMAC variant)
	md5	MD5 (HMAC variant)	
Authentication method	pre-share	Pre-shared key	Digital signature authentication
	rsa-sig	Digital signature authentication	
Diffie-Hellman group identifier	1	768-bit Diffie-Hellman group	768-bit Diffie-Hellman group
	2	1024-bit Diffie-Hellman group	
IKE SA lifetime	Null	1 minute to 1 day in seconds	1 day (86,400 seconds)

IKE tries to search for a consistent policy that exists on both peers when starting negotiation. One party that initiates negotiation sends all policies to the remote response party. The remote response party searches policies received from the remote peer by priority for a policy that matches a local policy.

When policies of both parties contain the same encryption algorithm, hash algorithm, authentication algorithm, and Diffie-Hellman parameter values and the lifetime of the policy on the remote peer is shorter than or equal to the lifetime of the compared policy, the shorter lifetime of the policy on the remote peer is used if no lifetime is specified. If no acceptable matched policy is found, IKE rejects negotiation and no IPSec SA is established. If a matched policy is found, IKE completes negotiation and establishes an IPSec SA.

Set parameters to balance between security and performance:

- Encryption algorithm: 56-bit DES-CBC, 168-bit 3DES-CBC, and 128-bit AES-CBC are currently supported.
- Hash algorithm: SHA-1 and MD5. The digest information generated when MD5 is used is less than that generated when SHA-1 is used, and MD5 is usually faster than SHA-1. It is proved that an attack targeted towards MD5 is successful but the attack method is very difficult. IKE can use the Hashed Message Authentication Code (HMAC) variant (MD5) to defend against such an attack.
- Authentication method: Currently, FSOS supports pre-shared key authentication and digital certificate authentication. In pre-shared key authentication, both parties need to configure correct pre-shared keys. In digital certificate authentication, both parties need to configure correct certificates (see the certificate configuration chapter).
- The Diffie-Hellman group identifier has two options: 768-bit Diffie-Hellman group, 1024-bit Diffie-Hellman group. It is difficult to attack the 1024-bit Diffie-Hellman group and the group occupies more CPU resources.
- IKE SA lifetime differs from IPSec SA lifetime. IKE SA lifetime refers to the validity period of IKE parameter negotiation and can be set to any value. As a universal rule, a shorter lifetime (reaching a critical point) indicates more secure IKE negotiation. If a longer lifetime is set, the negotiation of a new IPSec SA is faster.

Multiple IKE policies can be created, and each policy uses the combination of different parameter values. A unique priority (1-10000, with **1** indicating the highest priority) needs to be allocated to each created policy.

Multiple policies can be configured on each pair of peers. Among these policies, ensure that a policy must have the same encryption algorithm, hash algorithm, authentication algorithm, and Diffie-Hellman parameter values (the lifetime can be different) as a policy on the remote peer. If no policy is configured, the device uses the default policy, which is granted the lowest priority and uses the default value of each parameter.

The default policy and default values in configured policies are not displayed in the device configuration. To display the default policy and default values in configured policies, run the **show crypto isakmp policy** command.

By default, the system provides an IKE policy with the lowest priority. For the default configuration, see the chapters below.

Selecting Work Mode

There are two work modes: main mode and active mode (the default mode is main mode).

Configuring Local Identity

Selecting the work mode is specifying the work mode (main mode or active mode) for an initiator to initiate the first negotiation message. In main mode, the local identity configuration does not affect negotiation. In active mode, local identity configuration specifies the identity type in the first negotiation message of the initiator. It directly affects the negotiation in active mode. Currently, the local identity can be configured in three forms: local address; domain name; username@domain name.

By default, the negotiation of a pre-shared key uses an IP address as the ID while digital signature authentication uses the certificate DN as the ID. The digital signature authentication of devices from some other vendors uses an IP address as the ID. In this case, manually specify the ID type to ensure compatibility. There is a case in which the compatibility needs to be modified at the local peer due to the peer configuration. Default values can be used in other cases.

The configuration is valid globally and is not specific to a tunnel.

Configuring Automatic Identification of the Work Mode

A central device needs to support multiple dialup modes (some devices use main mode while some devices use active mode). The central device needs to respond to messages initiated in the two work modes and complete negotiation. Therefore, this command is used in such a work environment and has no effect on initiators.

By default, only negotiation in main mode can be identified because IDs are not protected in aggressive mode and the security in aggressive mode is poorer than that in main mode. Some devices use the aggressive mode for packet transmission by default. Automatic identification of the work mode needs to be configured to achieve compatibility.

Configuring Pre-shared Key

A pre-shared key is a key jointly owned by both peers that participate in IKE negotiation. Therefore, each pre-shared key maps to one pair of IKE peers. On a given peer, a key same as the key owned by multiple remote peers involved in sharing needs to be specified. For security, it is recommended to configure different keys between different peer pairs.

Negotiation of pre-shared keys must be configured. The certificate used in digital signature authentication contains public and private key pairs, which do not need to be configured.

Configuring DPD Detection

Currently, the Dead Peer Detection (DPD) is implemented using two mechanisms: on-demand mechanism and periodic mechanism. In on-demand mechanism, when packets are transmitted after the tunnel idle duration exceeds the configured time, the device is triggered to send a DPD detection message. In periodic mechanism, the device actively sends a DPD detection message after the tunnel idle duration exceeds the configured time. A DPD detection message can be retransmitted for a maximum of five times.

The DPD function is disabled by default. You can set parameters to enable the DPD function. It is recommended to enable the DPD function when the link is unstable.

Setting IKE Negotiation Rate

When thousands of tunnels are negotiated simultaneously, the negotiation fails to converge or the convergence is vslow. As a result, the entire negotiation takes several hours or even longer. To eliminate the deficiency, you can run this command to limit the negotiation rate, to ensure that the number of tunnels that are simultaneously involved in negotiation is controlled to a certain range and improve the negotiation efficiency.

The IKE negotiation rate limit function is enabled by default. The default rate limit is 1000, indicating that a maximum of 1000 tunnels can be simultaneously involved in negotiation. When a large number of tunnels are simultaneously involved in negotiation, if the default rate limit is adopted but the negotiation is still slow or fails, you can adjust the rate limit value. You can also run the **crypto isakmp limit disable** command to disable the negotiation rate limit function.

Setting NAT Traversal Timeout Parameter

The device complies with RFC3947 and uses the IPSEC NAT-T technology and UDP headers to resolve the NAT traversal problem. The keepalive mode is used for transmitting packets to prevent NAT connection timeout. The default time (5 minutes) is used when the NAT traversal timeout parameter is not set.

The NAT traversal function is automatically judged by the protocol and the default parameter value is provided. The value of the NAT traversal timeout parameter needs to be changed according to the NAT configuration. When no data is transmitted, the keepalive mode ensures that the NAT records are effective, to prevent tunnel data transmission interruption caused by interface re-assignment during NAT re-establishment.

10.4 Configuration

Configuration	Description and Command	
Configuring IKE	**crypto isakmp enable**	Enables or disables IKE.
	crypto isakmp policy *priority*	Creates an IKE policy.
	self-identity	Configures the local identity.
	crypto isakmp mode-detect	Configures automatic identification of the work mode.
	crypto isakmp key	Configures a pre-shared key.
	crypto isakmp keepalive	Configures DPD detection.
	crypto isakmp limit rate	Sets the IKE negotiation rate.
	crypto isakmp nat	Sets the NAT traversal timeout parameter.

10.4.1 Configuring IKE

Configuration Effect

- Configure an IKE negotiation policy.

Notes

- The priorities of IKE policies are sorted by the policy number.
- The default policy number is 65535 and the default policy is used when no policy is configured.

Configuration Steps

(Optional) Enabling or Disabling IKE

- Ensure that IKE is working and is not disabled.
- The IKE function is enabled by default. It can be disabled using a command in special cases.

Ensuring Compatibility Between ACL and IKE

- If an ACL is configured on the device, ensure that the device does not prohibit IKE communication data.
- If a conflict causes an abnormality in forwarding of tunnel data and the system cannot identify the abnormality, configuration personnel needs to ensure the compatibility between ACL and IKE.

Creating IKE Policy

- Specify parameters used by IKE. An IKE policy is configured globally.
- By default, the system provides an IKE policy with the lowest priority. For the default configuration, see the chapters below.

Selecting Work Mode

- IKE supports two work modes during IKE negotiation: main mode and active mode (active mode is also called aggressive mode in some documents).
- In aggressive mode, IDs are not protected and fewer packets are involved in negotiation. Select a proper work mode as required.

(Optional) Configuring Local Identity

- Configure the local identity for IKE negotiation.
- By default, the negotiation of a pre-shared key uses an IP address as the ID while digital signature authentication uses the certificate DN as the ID. The digital signature authentication of devices from some other vendors uses an IP address as the ID. In this case, manually specify the ID type to ensure compatibility. There is a case in which the compatibility needs to be modified at the local peer due to the peer configuration. Default values can be used in other cases.
- The configuration is valid globally and is not specific to a tunnel.

(Optional) Configuring Automatic Identification of the Work Mode

- Configure whether the response party of IKE negotiation automatically accepts negotiation in active mode.
- By default, only negotiation in main mode can be identified because IDs are not protected in aggressive mode and the security in aggressive mode is poorer than that in main mode. Some devices use the aggressive mode for packet transmission by default. Automatic identification of the work mode needs to be configured to achieve compatibility.

Configuring Pre-shared Key

- Configure the joint key between IKE peers. A pre-shared key can be configured for a specific IP address or domain name. Wildcard keys are supported.
- Negotiation of pre-shared keys must be configured. The certificate used in digital signature authentication contains public and private key pairs, which do not need to be configured.

(Optional) Configuring DPD Detection

- DPD detection can be configured in two modes: on-demand mode and periodic mode. It detects whether the peer device functions properly and eliminates tunnel vulnerabilities.
- The DPD function is disabled by default. You can set parameters to enable the DPD function. It is recommended to configure the DPD function when the link is unstable.

(Optional) Setting IKE Negotiation Rate

- Setting the IKE negotiation rate can effectively prevent a negotiation failure or long negotiation duration caused by simultaneous negotiation of a large number of tunnels.
- The IKE negotiation rate limit function is enabled by default. The default rate limit is 1000, indicating that a maximum of 1000 tunnels can be simultaneously involved in negotiation. When a large number of tunnels are simultaneously involved in negotiation, if the default rate limit is adopted but the negotiation is still slow or fails, you can adjust the rate limit value. You can also run the **crypto isakmp limit disable** command to disable the negotiation rate limit function.

(Optional) Setting NAT Traversal Timeout Parameter

- The NAT-T technology uses a UDP header to resolve NAT transversal problem. Keepalive packets need to be used to ensure the persistency of the UDP connection, to prevent NAT connection timeout.
- The NAT traversal function is automatically judged by the protocol and the default parameter value is provided. The value of the NAT traversal timeout parameter needs to be changed according to the NAT configuration. When no data is transmitted, the keepalive mode ensures that the NAT records are effective, to prevent tunnel data transmission interruption caused by interface re-assignment during NAT re-establishment.

Verification

- Run the **show crypto policy** command to check the configuration integrity and whether the configuration is consistent with the peer configuration.

Related Commands

(Optional) Enabling or Disabling IKE

Command	**crypto isakmp enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	IKE is enabled by default. If you need to use IKE to negotiate IPSec SAs, this command is not required. If you do not use IKE to negotiate IPSec SAs, use the **no** form of this command to

	disable IKE.

Creating IKE Policy

Command	**crypto isakmp policy** *priority*
Parameter Description	*priority*: Indicates the priority.
Command Mode	Global configuration mode
Usage Guide	Use this command to specify parameters for negotiating IKE SAs. Run this command to enter the IKE policy configuration mode. In IKE policy configuration mode, you can set the following parameters: encryption(IKE policy): The default value is 56-bit DES-CBC. hash(IKE policy): The default value is SHA-1. authentication(IKE policy): The default value is RSA signature. group(IKE policy): The default value is 768-bit group. Diffie-Hellman lifetime(IKE policy): The default value is 86,400 seconds (1 day). If a parameter is not set, the default value of the parameter will be used. You can configure multiple IKE policies on the device. After the IKE negotiation starts, the device tries to find out the public policy configured at both ends, and the search starts from the policy with the highest priority on the remote peer.

Command	**encryption des | 3des | aes-128 | aes-192 | aes-256**
Parameter Description	des: Specifies the 56-bit DES-CBC as the encryption algorithm. 3des: Specifies the 168-bit 3DES-CBC as the encryption algorithm. aes-128: Specifies the AES with the 128-bit key as the encryption algorithm. aes-192: Specifies the AES with the 192-bit key as the encryption algorithm. aes-256: Specifies the AES with the 256-bit key as the encryption algorithm.
Command Mode	IKE policy configuration mode
Usage Guide	The data encryption algorithm specified by this command is used for encryption of IKE SA data. It differs from the encryption algorithm used by IPSec SAs. The DES encryption algorithm is used by default.

Command	**hash** {**sha** | **md5**}
Parameter Description	sha: Specifies SHA-1 (HMAC variant) as the hash algorithm. md5: Specifies MD5 (HMAC variant) as the hash algorithm.
Command Mode	IKE policy configuration mode
Usage Guide	Use this command to specify the hash algorithm used in an IKE policy. The SHA algorithm is used by default.

Command	**authentication** {**pre-share | rsa-sig**}

Parameter Description	pre-share: Indicates a pre-shared key. rsa-sig: Indicates the digital certificate.
Command Mode	IKE policy configuration mode
Usage Guide	Currently, the authentication mode in an IKE negotiation policy uses the digital signature by default, which is the same as the authentication mode in Cisco devices. If you need to use pre-shared key authentication mode, you need to add an IKE policy, in which the pre-shared key authentication needs to be configured.

Command	**group** { **1** | **2** }
Parameter Description	**1**: Specifies 768-bit Diffie-Hellman group. **2**: Specifies 1024-bit Diffie-Hellman group. **5**: Specifies 1536-bit Diffie-Hellman group.
Command Mode	IKE policy configuration mode
Usage Guide	Use this command to specify the group applied in the IKE policy. By default, **group 1** is specified.

Command	**lifetime** *seconds*
Parameter Description	*seconds*: Indicates the IKE tunnel timeout time.
Command Mode	IKE policy configuration mode
Usage Guide	Use this command to specify the lifetime of IKE SAs. When starting negotiation, IKE first reaches an agreement on session security parameters with the peer IKE. These consistent parameters will be referenced by IKE SAs on each peer and are retained on each peer till the IKE SA lifetime times out. A new SA must be negotiated prior to the expiration of the current SA. IPSec SAs are negotiated on the basis of IKE SAs. Therefore, a longer lifetime should be configured for IKE SAs to shorten the time required for negotiating IPSec SAs. However, the cracking probability is directly proportional to the lifetime. A longer lifetime indicates a higher cracking probability whereas a shorter lifetime indicates a lower cracking probability. Therefore, set a proper lifetime (for example, half a day) as required. The default value is **86,400** seconds.

Selecting Work Mode

Command	**set exchange-mode** { **main** | **aggressive** }
Parameter Description	main: Indicates the main mode. aggressive: Indicates the aggressive mode.
Command Mode	Encryption mapping configuration mode
Usage Guide	The IKE negotiation includes two phases: In Phase 1, a secure channel that passes authentication is established between two ISAKMP entities. The main mode or active mode can be adopted in this phase. In Phase 2, service SAs are negotiated.

	Select the required work mode in Phase 1 based on their advantages and disadvantages. The main mode is adopted by default. When IP addresses are not statically configured, the active mode is recommended.

(Optional) Configuring Local Identity

Command	**self-identity** { **address** | **trustpoint** *trustpoint* | **fqdn** *fqdn* | **user-fqdn** *user-fqdn* }
Parameter Description	self-identity: Indicates the local ID type and name. address: Indicates the local IP address. trustpoint: Specifies the local certificate. fqdn: Uses the full domain name. user-fqdn: Uses the email address.
Command Mode	Global configuration mode
Usage Guide	Set the identity for the negotiation initiated in active mode. You can use the domain name or address to specify the local identity.

(Optional) Configuring Automatic Identification of Work Mode

Command	**Crypto isakmp mode-detect**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Many vendors set foot in security products but the implementation methods of security products from different vendors are different. Two work modes are supported in Phase 1 of IKE negotiation. To ensure compatibility, use this command to complete negotiation in active mode when the IKE negotiation initiated by the peer cannot be completed.

Configuring Pre-shared Key

Command	**crypto isakmp key** { **0** | **7** } *keystring* { **hostname** *peer-hostname* | **address** *peer-address* [*mask*] }
Parameter Description	address: Specifies the address that uses the key. hostname: Specifies the domain name that uses the key.
Command Mode	Global configuration mode
Usage Guide	In general, IKE uses a pre-shared key for negotiation. To enable IKE to successfully establish IKE SAs, you must use this command to configure the same pre-shared key on both communication peers. If the specified peer is a network segment, use **mask** to identify the subnet mask. When both **peer-address** and **Mask** are **0.0.0.0**, the default pre-shared key is used.

(Optional) Configuring DPD Detection

Command	**crypto isakmp keepalive** *seconds* [*retries*] [**on-demand** | **periodic**]
Parameter Description	*seconds*: Indicates the detection duration. *retries*: Indicates the detection interval. periodic: Indicates the interval mode. on-demand: Indicates the packet triggering mode.

Command Mode	Global configuration mode
Usage Guide	DPD detection is disabled by default. Extra overheads can be reduced in packet triggering mode. In periodic mode, the response is faster. Therefore, select a proper detection mode as required.

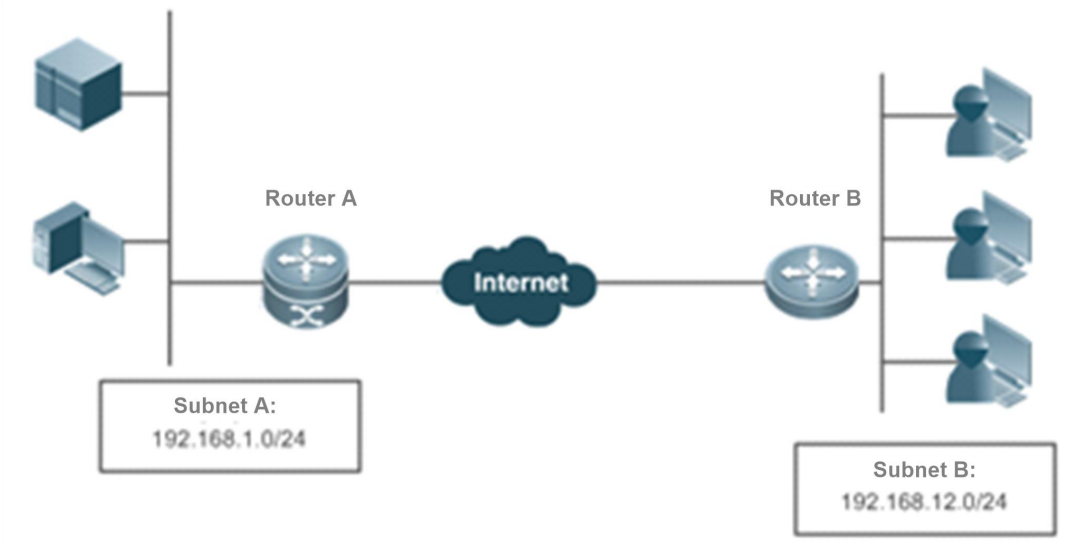
Setting IKE Negotiation Rate

Command	**crypto isakmp limit rate** *numbers*
Parameter Description	*numbers*: Indicates the rate limit.
Command Mode	Global configuration mode
Usage Guide	The rate limit function is enabled by default. The default rate limit is 1000. Change the value as required or run the **crypto isakmp limit disable** command to disable the rate limit function.

(Optional) Setting NAT Traversal Timeout Parameter

Command	**Crypto isakmp nat keepalive** *secs*
Parameter Description	*secs:* Indicates the interval for sending keepalive packets.
Command Mode	Global configuration mode
Usage Guide	The device complies with RFC3947 and uses the IPSEC NAT-T technology and UDP headers to resolve the NAT traversal problem. The keepalive mode is used for transmitting packets to prevent NAT connection timeout. Run the **crypto isakmp nat keepalive** command to specify the interval for sending keepalive messages. If the interval is not specified, the default value (5 minutes) is used.

Configuration Example

Scenario Figure 10-3	
	The IP data communication between two subnets needs to be protected. FS Router A is used as a central gateway and connects to Subnet A. FS Router B is used as a branch gateway and connects

	to Subnet B. The implementation requirements are as follows: ● The tunnel mode is used. ● The protection mode is ESP-DES-MD5 (providing encryption and authentication services). ● The IP address of the WAN interface on Router A is fixed to 202.1.1.2/24 and the WAN interface is connected to the Internet over a dedicated line. ● Router B connects to the Internet over PPPoE through the ADSL and the IP address of Router B is dynamically assigned by the ISP. ● The pre-shared key is used and the central router uses the host name to specify the pre-shared key. ● IKE is used to establish SAs.
Configuration Steps Router A	● An IPSec VPN tunnel is a point-to-point encryption tunnel. Devices at both ends of the tunnel encrypt and decrypt data via the negotiated key. IKE needs to be configured before an IPSec VPN tunnel is established. **Configuration on Router A:** # Define an IKE policy, in which the authentication method uses the pre-shared key and other parameters use default values. FS(config)#crypto isakmp policy 1 FS(isakmp-policy)#authentication pre-share # Configure the default pre-shared key. The IP address of the peer is dynamically assigned. Therefore, specify the host name to search for the pre-shared key. FS(config)#crypto isakmp key 0 preword hostname www.google.com # Configure the automatic identification of the work mode on the central router. FS(config)#crypto isakmp mode-detect # Define a transformation set. FS(config)#crypto ipsec transform-set myset esp-des esp-md5-hmac # Define dynamic encryption mapping. FS(config)#crypto dynamic-map dymymap 5 FS(config-crypto-map)#set transform-set myset FS(config-crypto-map)#match address 101 # Add a dynamic encryption mapping set to the static encryption mapping set. FS(config)#crypto map mymap 10 ipsec-isakmp dynamic dymymap FS(config)#interface GigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)#ip address 192.168.1.1 255.255.255.0 # Apply the encryption mapping set to an interface. FS(config)#interface serial 0 FS(config-if-serial 0)#ip address 202.1.1.2 255.255.255.0 FS(config-if-serial 0)#encapsulation ppp FS(config-if-serial 0)#crypto map mymap FS(config)#ip route 0.0.0.0 0.0.0.0 Serial0

Define an encryption access list to protect the IP communication between the subnet 192.168.1.0/24 and the subnet 192.168.12.0/24.

```
FS(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.12.0 0.0.0.255
```

Configuration on Router B:

Enable IKE.

```
FS(config)#crypto isakmp enable
```

Configure the local identity.

```
FS(config)#self-identity fqdn www.google.com
```

Define an IKE policy, in which the authentication method uses the pre-shared key and other parameters use default values.

```
FS(config)#crypto isakmp policy 1
FS(isakmp-policy)#authentication pre-share
```

Configure a pre-shared key and transformation set.

```
FS(config)#crypto isakmp key 0 preword address 202.1.1.2
FS(config)#crypto ipsec transform-set myset    esp-des esp-md5-hmac
```

Define an encryption mapping set.

```
FS(config)#crypto map mymap 5 ipsec-isakmp
FS(config-crypto-map)#set peer 202.1.1.2
FS(config-crypto-map)#set exchange-mode aggressive
FS(config-crypto-map)#set transform-set myset
FS(config-crypto-map)#match address 101
FS(config)#interface GigabitEthernet 0/0
FS(config-if-GigabitEthernet 0/0)#ip address 192.168.12.1 255.255.255.0
FS(config)#interface GigabitEthernet 0/1
FS(config-if-GigabitEthernet 0/1)#no ip addrsss
FS(config-if-GigabitEthernet 0/1)#pppoe enable
FS(config-if-GigabitEthernet 0/1)#pppoe-client 1 dial-pool-number 1 dial-on-demand
```

Apply the encryption mapping set to an interface.

```
FS(config)#interface dialer 0
FS(config-if-dialer 0)#mtu 1488
FS(config-if-dialer 0)#ip address negotiate
FS(config-if-dialer 0)#encapsulation ppp
FS(config-if-dialer 0)#ppp pap sent-username xxx password xxx
FS(config-if-dialer 0)#crypto map mymap
FS(config-if-dialer 0)#dialer idle-timeout 2400
FS(config-if-dialer 0)#dialer pool 1
FS(config-if-dialer 0)#dialer-group 1
FS(config)#dialer-list protocol ip permit
FS(config)#ip route 0.0.0.0 0.0.0.0 Dialer0 permanent
```

Define an encryption access list to protect the IP communication between the subnet

	192.168.12.0/24 and the subnet 192.168.1.0/24. FS(config)#access-list 101 permit ip 192.168.12.0 0.0.0.255 192.168.1.0 0.0.0.255

10.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears IKE connections.	**clear crypto isakmp** [*connection-id*]
Clears IPSec VPN login and logout logs.	**clear crypto log**

Displaying

Description	Command
Displays all IKE policy parameters.	**show crypto isakmp policy**
Displays all current IKE SAs.	**show crypto isakmp sa**
Displays all IPSec VPN login and logout logs.	**show crypto log**

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs IKE events.	**debug crypto isakmp**

11 Configuring ITBOX

11.1 Overview

ITBOX is a store information management platform launched by FS Network for resolving the chain store information management issues.

Users in each store only need to scan the QR code provided by the headquarters during first deployment and set the WAN port and basic store information. Then, VPN configuration is automatically delivered to ITBOX in the store. In this way, common users can perform quick deployment.

Access points (APs) in all stores are managed and controlled by the headquarters. Any configuration change resulted from changes of the topology or VPN configuration in the headquarters is automatically delivered to stores, without separately notifying each store of the change. This reduces the store operation and maintenance costs, and realizes one-off deployment of store APs.

11.2 Applications

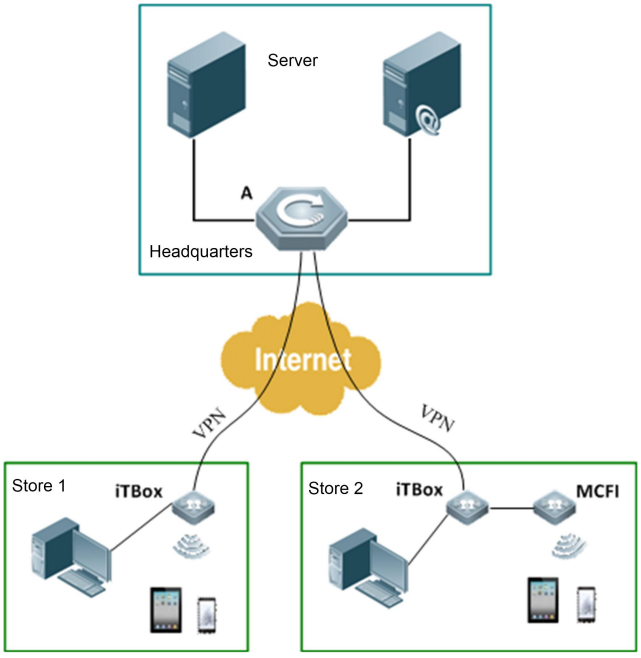
Application	Description
Applying ITBOX	The headquarters egress gateway serves as the server to provide the centralized management service for branches.

11.2.1 Applying ITBOX

Scenario

In Figure 11-1, A serves as the headquarters egress gateway, with the VPN service enabled. ITBOX in each store serves as the VPN client to set up a VPN channel with the headquarters egress gateway.

Figure 11-1



Remarks	A is the egress gateway.

Deployment

- Enable the VPN service on A.
- Enable the Web service on A.
- Equip branches with VPN clients.

11.3 Features

Overview

Feature	Description
Easy Deployment at Branches	Implements quick deployment and configuration of VPNs at branches.
Centralized Management of Branches	Implements centralized management on the VPN, Wi-Fi, bandwidth assurance, login password, and the like of branches.
Branch Status Monitoring	Monitors statuses of the VPN, LAN port, and the like, and displays information such as the number of online clients and interface traffic at branches.

11.3.1 Easy Deployment at Branches

No VPN configuration is required, which implements quick deployment at branches.

Working Principle

After the headquarters egress gateway is configured, a QR code is generated, which includes information such as the IP address of the headquarters egress gateway and login code.

After the mobile phone connects to the wireless network at a branch and scans the QR code, parameters for connecting to the headquarters egress gateway are automatically configured. Meanwhile, the mobile phone displays a Web configuration page. Users can set the basic branch information and WAN port to complete branch deployment. The branch immediately sets up a connection to the headquarters egress gateway and receives configuration information such as the VPN and Wi-Fi settings from the headquarters.

11.3.2 Centralized Management of Branches

The headquarters egress gateway performs centralized management on the VPN, Wi-Fi, bandwidth assurance, login password, and the like of branches. The headquarters delivers the configuration information directly to all branches in a unified manner, and the branches do not need to perform configuration separately.

Working Principle

The headquarters enables TCP Port 11701 and waits for the branch to set up the connection. After the connection is set up, the headquarters delivers the Shell script to the branch via this connection. The headquarters delivers the preset configuration script immediately after the connection is set up. If the configuration is modified, the modified configuration script is also delivered from the headquarters to branches via this connection.

11.3.3 Branch Status Monitoring

The headquarters monitors the VPN connection status and LAN port power-on status at branches. The headquarters can also query information such as the number of online clients and interface traffic at specified branches.

Working Principle

The headquarters periodically delivers the Shell script to branches, collects information such as the VPN status and LAN port power-on status, and provides query interfaces to display branches with VPN connection exceptions and with a concerned LAN port not in the UP state. The headquarters can also deliver the shell script to specified branches to display the information such as the number of online clients and interface traffic.

11.4 Configuration

Configuration	Description and Command	
Upgrading System Version at Branches	(Optional) It is used to upgrade the system version at branches.	
	evpn-server version	Configures the product type and version number of the system to be upgraded.
Delivering Configuration to Branches	(Optional) It is used to manage the branch configuration.	
	evpn-server shell all clients file	Delivers the configuration file.

11.4.1 Upgrading System Version at Branches

Configuration Effect

- Upgrade systems for branches with a specified product type.

Notes

Before configuration, rename the upgrade package as iTBox.tgz and place the upgrade package to the **/mnt/sata0/evpn** sub directory.

Configuration Steps

Setting Up IP Address and Web Access Port of Headquarters

- Mandatory.
- Run this command to generate the URL for downloading the upgrade package.

Command	evpn-server outside-ip *A.B.C.D* web-port port
Parameter Description	*A.B.C.D:* Indicates the Web server address (public IP address of the device). *port:* Indicates the Web access port.
Defaults	N/A
Command	Global configuration mode

Mode	
Usage Guide	N/A

Setting Version Number of Specified Product

- Mandatory.

Command	evpn-server version *product version*
Parameter Description	*product:* Indicates the product name. *version:* Indicates the system version number.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **evpn-server shell** command to check the system version number at the branch after the upgrade is completed.

Configuration Example

Upgrading FS-MA1220-I System to 1.0.0.1114

Configuration Steps	- Set the product version of FS-MA1220-I to 1.0.0.1114.
	FS(config)# evpn-server outside-ip 172.18.124.100 web-port 80 FS(config)# evpn-server version FS-MA1220-I 1.0.0.1114
Verification	- Run the **evpn-server shell** command to check the system version number at the branch after the upgrade is completed.
	FS# evpn-server shell sn G1HD927000001 string "cat /proc/rg_sys/software_version" with-result 1.0.0.1114 FS#

11.4.2 Delivering Configuration to Branches

Configuration Effect

- Deliver configuration to branches.

Notes

Generate the configuration script for branches in advance on the egress gateway.

Configuration Steps

Delivering Configuration to Branches

- Mandatory.

Command	**evpn-server shell all-clients file** *path*
Parameter Description	*path:* Indicates the path for storing the configuration file.
Defaults	-
Command Mode	Privileged EXEC mode
Usage Guide	-

Verification

- Check whether the configuration on the branch device takes effect.

Configuration Example

Configuring VPN at Branches

Configuration Steps	● Deliver VPN configuration to the branch.
	FS# evpn shell all file "/data/evpn/cfg_vpn.sh.text"
Verification	● Check whether the VPN configuration at the branch takes effect.

11.5 Monitoring

Displaying

Description	Command
Displays branch status statistics.	**show evpn-server client info**
Displays branches that request for connections.	**show evpn-server client new**
Displays branches with the device offline.	**show evpn-server client offline**
Displays branches with the device online.	**show evpn-server client online**
Displays branches with port exceptions.	**show evpn-server client port-off**
Displays specified branches.	**show evpn-server client sn**
Displays branches with VPN exceptions.	**show evpn-server client vpn-off**
Displays branches with normal VPNs.	**show evpn-server client vpn-on**
Displays current configuration.	**show evpn-server config**

12 Configuring AAA

12.1 Overview

Authentication, authorization, and accounting (AAA) provides a unified framework for configuring the authentication, authorization, and accounting services. FS Networks devices support the AAA application.

AAA provides the following services in a modular way:

Authentication: Refers to the verification of user identities for network access and network services. Authentication is classified into local authentication and authentication through Remote Authentication Dial In User Service (RADIUS) and Terminal Access Controller Access Control System+ (TACACS+).

Authorization: Refers to the granting of specific network services to users according to a series of defined attribute-value (AV) pairs. The pairs describe what operations users are authorized to perform. AV pairs are stored on network access servers (NASs) or remote authentication servers.

Accounting: Refers to the tracking of the resource consumption of users. When accounting is enabled, NASs collect statistics on the network resource usage of users and send them in AV pairs to authentication servers. The records will be stored on authentication servers, and can be read and analyzed by dedicated software to realize the accounting, statistics, and tracking of network resource usage.

AAA is the most fundamental method of access control. FS Networks also provides other simple access control functions, such as local username authentication and online password authentication. Compared to them, AAA offers higher level of network security.

AAA has the following advantages:

- Robust flexibility and controllability
- Scalability
- Standards-compliant authentication
- Multiple standby systems

12.2 Applications

Application	Description
Configuring AAA in a Single-Domain Environment	AAA is performed for all the users in one domain.
Configuring AAA in a Multi-Domain Environment	AAA is performed for the users in different domains by using different methods.

12.2.1 Configuring AAA in a Single-Domain Environment

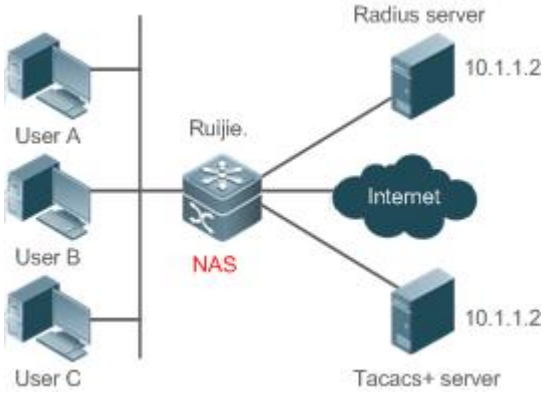
Scenario

In the network scenario shown in Figure 12- 1, the following application requirements must be satisfied to improve the security management on the NAS:

18. To facilitate account management and avoid information disclosure, each administrator has an individual account with different username and password.

19. Users must pass identity authentication before accessing the NAS. The authentication can be in local or centralized mode. It is recommended to combine the two modes, with centralized mode as active and local mode as standby. As a result, users must undergo authentication by the RADIUS server first. If the RADIUS server does not respond, it turns to local authentication.
20. During the authentication process, users can be classified and limited to access different NASs.
21. Permission management: Users managed are classified into Super User and Common User. Super users have the rights to view and configure the NAS, and common users are only able to view NAS configuration.
22. The AAA records of users are stored on servers and can be viewed and referenced for auditing. (The TACACS+ server in this example performs the accounting.)

Figure 12-1



Remarks	User A, User B, and User C are connected to the NAS in wired or wireless way. The NAS is an access or convergence switch. The RADIUS server can be the Windows 2000/2003 Server (IAS), UNIX system component, and dedicated server software provided by a vendor. The TACACS+ server can be the dedicated server software provided by a vendor.

Deployment

- Enable AAA on the NAS.
- Configure an authentication server on the NAS.
- Configure local users on the NAS.
- Configure the authentication service on the NAS.
- Configure the authorization service on the NAS.
- Configure the accounting service on the NAS.

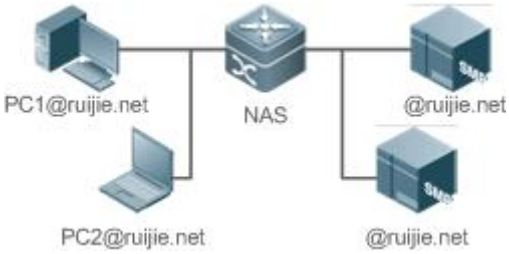
12.2.2 Configuring AAA in a Multi-Domain Environment

Scenario

Configure the domain-based AAA service on the NAS.

- A user can log in by entering the username PC1@FS.net or PC2@FS.com.cn and correct password on an 802.1X client.
- Permission management: Users managed are classified into Super User and Common User. Super users have the rights to view and configure the NAS, and common users are only able to view NAS configuration.
- The AAA records of users are stored on servers and can be viewed and referenced for auditing.

Figure 12-2



Remarks	The clients with the usernames **PC1@FS.net** and **PC2@FS.com.cn** are connected to the NAS in wired or wireless way. The NAS is an access or convergence switch. The Security Accounts Manager (SAM) server is a universal RADIUS server provided by FS Networks.

Deployment

- Enable AAA on the NAS.
- Configure an authentication server on the NAS.
- Configure local users on the NAS.
- Define an AAA method list on the NAS.
- Enable domain-based AAA on the NAS.
- Create domains and AV sets on the NAS.

12.3 Features

Basic Concepts

Local Authentication and Remote Server Authentication

Local authentication is the process where the entered passwords are verified by the database on the NAS.

Remote server authentication is the process where the entered passwords are checked by the database on a remote server. It is mainly implemented by the RADIUS server and TACACS+ server.

Method List

AAA is implemented using different security methods. A method list defines a method implementation sequence. The method list can contain one or more security protocols so that a standby method can take over the AAA service when the first method fails. On FS devices, the first method in the list is tried in the beginning and then the next is tried one by one if the previous gives no response. This method selection

process continues until a security method responds or all the security methods in the list are tried out. Authentication fails if no method in the list responds.

A method list contains a series of security methods that will be queried in sequence to verify user identities. It allows you to define one or more security protocols used for authentication, so that the standby authentication method takes over services when the active security method fails. On FS devices, the first method in the list is tried in the beginning and then the next is tried one by one if the previous gives no response. This method selection process continues until a method responds or all the methods in the method list are tried out. Authentication fails if no method in the list responds.

The next authentication method proceeds on FS devices only when the current method does not respond. When a method denies user access, the authentication process ends without trying other methods.

Figure 12-3

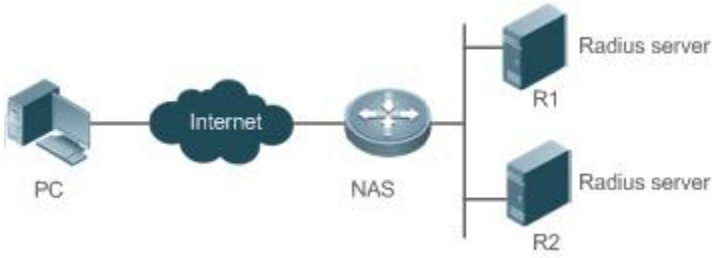


Figure 12-3 shows a typical AAA network topology, where two RADIUS servers (R1 and R2) and one NAS are deployed. The NAS can be the client for the RADIUS servers.

Assume that the system administrator defines a method list, where the NAS selects R1 and R2 in sequence to obtain user identity information and then accesses the local username database on the server. For example, when a remote PC user initiates dial-up access, the NAS first queries the user's identity on R1. When the authentication on R1 is completed, R1 returns an Accept response to the NAS. Then the user is permitted to access the Internet. If R1 returns a Reject response, the user is denied Internet access and the connection is terminated. If R1 does not respond, the NAS considers that the R1 method times out and continues to query the user's identity on R2. This process continues as the NAS keeps trying the remaining authentication methods, until the user request is authenticated, rejected, or terminated. If all the authentication methods are responded with Timeout, authentication fails and the connection will be terminated.

The Reject response is different from the Timeout response. The Reject response indicates that the user does not meet the criteria of the available authentication database and therefore fails in authentication, and the Internet access request is denied. The Timeout response indicates that the authentication server fails to respond to the identity query. When detecting a timeout event, the AAA service proceeds to the next method in the list to continue the authentication process.

This document describes how to configure AAA on the RADIUS server. For details about the configuration on the TACACS+ server, see the *Configuring TACACS+*.

AAA Server Group

You can define an AAA server group to include one or more servers of the same type. If the server group is referenced by a method list, the NAS preferentially sends requests to the servers in the referenced server group when the method list is used to implement AAA.

Overview

Feature	Description
AAA Authentication	Verifies whether users can access the Internet.
AAA Authorization	Determines what services or permissions users can enjoy.
AAA Accounting	Records the network resource usage of users.
Multi-Domain AAA	Creates domain-specific AAA schemes for 802.1X stations (STAs) in different domains.

12.3.1 AAA Authentication

Authentication, authorization, and accounting are three independent services. The authentication service verifies whether users can access the Internet. During authentication, the username, password, and other user information are exchanged between devices to complete users' access or service requests. You can use only the authentication service of AAA.

To configure AAA authentication, you need to first configure an authentication method list. Applications perform authentication according to the method list. The method list defines the types of authentication and the sequence in which they are performed. Authentication methods are implemented by specified applications. The only exception is the default method list. All applications use the default method list if no method list is configured.

AAA Authentication Scheme

- No authentication (**none**)

The identity of trusted users is not checked. Normally, the no-authentication (None) method is not used.

- Local authentication (**local**)

Authentication is performed on the NAS, which is configured with user information (including usernames, passwords, and AV pairs). Before local authentication is enabled, run the **username password** command to create a local user database.

- Remote server group authentication (**group**)

Authentication is performed jointly by the NAS and a remote server group through RADIUS or TACACS+. A server group consists of one or more servers of the same type. User information is managed centrally on a remote server, thus realizing multi-device centralized and unified authentication with high capacity and reliability. You can configure local authentication as standby to avoid authentication failures when all the servers in the server group fail.

AAA Authentication Types

FS products support the following authentication types:

- Login authentication

Users log in to the command line interface (CLI) of the NAS for authentication through Secure Shell (SSH), Telnet, and File Transfer Protocol (FTP).

- Enable authentication

After users log in to the CLI of the NAS, the users must be authenticated before CLI permission update. This process is called Enable authentication (in Privileged EXEC mode).

- Point-to-Point Protocol (PPP) authentication

PPP authentication is performed for users that initiate dial-up access through PPP.

- iPortal (built-in portal) authentication

iPortal authentication is performed by the first generation portal server.

Related Configuration

Enabling AAA

By default, AAA is disabled.

To enable AAA, run the **aaa new-model** command.

Configuring an AAA Authentication Scheme

By default, no AAA authentication scheme is configured.

Before you configure an AAA authentication scheme, determine whether to use local authentication or remote server authentication. If the latter is to be implemented, configure a RADIUS or TACACS+ server in advance. If local authentication is selected, configure the local user database information on the NAS.

Configuring an AAA Authentication Method List

By default, no AAA authentication method list is configured.

Determine the access mode to be configured in advance. Then configure authentication methods according to the access mode.

12.3.2 AAA Authorization

AAA authorization allows administrators to control the services or permissions of users. After AAA authorization is enabled, the NAS configures the sessions of users according to the user configuration files stored on the NAS or servers. After authorization, users can use only the services or have only the permissions permitted by the configuration files.

AAA Authorization Scheme

- Direct authorization (**none**)

Direct authorization is intended for highly trusted users, who are assigned with the default permissions specified by the NAS.

- Local authorization (**local**)

Local authorization is performed on the NAS, which authorizes users according to the AV pairs configured for local users.

- Remote server-group authorization (**group**)

Authorization is performed jointly by the NAS and a remote server group. You can configure local or direct authorization as standby to avoid authorization failures when all the servers in the server group fail.

AAA Authorization Types

- EXEC authorization

After users log in to the CLI of the NAS, the users are assigned with permission levels (0 to 15).

- Config-commands authorization

Users are assigned with the permissions to run specific commands in configuration modes (including the global configuration mode and sub-modes).

- Console authorization

After users log in through consoles, the users are authorized to run commands.

- Command authorization

Authorize users with commands after login to the CLI of the NAS.

- Network authorization

After users access the Internet, the users are authorized to use the specific session services. For example, after users access the Internet through PPP and Serial Line Internet Protocol (SLIP), the users are authorized to use the data service, bandwidth, and timeout service.

Related Configuration

Enabling AAA

By default, AAA is disabled.

To enable AAA, run the **aaa new-model** command.

Configuring an AAA Authorization Scheme

By default, no AAA authorization scheme is configured.

Before you configure an AAA authorization scheme, determine whether to use local authorization or remote server-group authorization. If remote server-group authorization needs to be implemented, configure a RADIUS or TACACS+ server in advance. If local authorization needs to be implemented, configure the local user database information on the NAS.

Configuring an AAA Authorization Method List

By default, no AAA authorization method list is configured.

Determine the access mode to be configured in advance. Then configure authorization methods according to the access mode.

12.3.3 AAA Accounting

In AAA, accounting is an independent process of the same level as authentication and authorization. During the accounting process, start-accounting, update-accounting, and end-accounting requests are sent to the configured accounting server, which records the network resource usage of users and performs accounting, audit, and tracking of users' activities.

In AAA configuration, accounting scheme configuration is optional.

AAA Accounting Schemes

- No accounting (**none**)

Accounting is not performed on users.

- Local accounting (**local**)

Accounting is completed on the NAS, which collects statistics on and limits the number of local user connections. Billing is not performed.

- Remote server-group accounting (**group**)

Accounting is performed jointly by the NAS and a remote server group. You can configure local accounting as standby to avoid accounting failures when all the servers in the server group fail.

AAA Accounting Types

- EXEC accounting

Accounting is performed when users log in to and out of the CLI of the NAS.

- Command accounting

Records are kept on the commands that users run on the CLI of the NAS.

- Network accounting

Records are kept on the sessions that users set up after completing 802.1X and Web authentication to access the Internet.

Related Configuration

Enabling AAA

By default, AAA is disabled.

To enable AAA, run the **aaa new-model** command.

Configuring an AAA Accounting Scheme

By default, no AAA accounting method is configured.

Before you configure an AAA accounting scheme, determine whether to use local accounting or remote server-group accounting. If remote server-group accounting needs to be implemented, configure a RADIUS or TACACS+ server in advance. If local accounting needs to be implemented, configure the local user database information on the NAS.

Configuring an AAA Accounting Method List

By default, no AAA accounting method list is configured.

Determine the access mode to be configured in advance. Then configure accounting methods according to the access mode.

12.3.4 Multi-Domain AAA

In a multi-domain environment, the NAS can provide the AAA services to users in different domains. The user AVs (such as usernames and passwords, service types, and permissions) may vary with different domains. It is

necessary to configure domains to differentiate the user AVs in different domains and configure an AV set (including an AAA service method list, for example, RADIUS) for each domain.

Our products support the following username formats:

1. userid@domain-name
2. domain-name\userid
3. userid.domain-name
4. userid

The fourth format (userid) does not contain a domain name, and it is considered to use the **default** domain name.

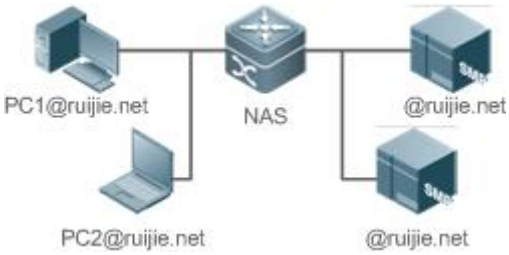
The NAS provides the domain-based AAA service based on the following principles:

- Resolves the domain name carried by a user.
- Searches for the user domain according to the domain name.
- Searches for the corresponding AAA method list name according to the domain configuration information on the NAS.
- Searches for the corresponding method list according to the method list name.
- Provides the AAA services based on the method list.

If any of the preceding procedures fails, the AAA services cannot be provided.

Figure 12-4 shows the typical multi-domain topology.

Figure 12-4



Related Configuration

Enabling AAA

By default, AAA is disabled.

To enable AAA, run the **aaa new-model** command.

Configuring an AAA Method List

By default, no AAA method list is configured.

For details, see section 5.2.1, section 5.2.2, and section 5.2.3.

Enabling the Domain-Based AAA Service

By default, the domain-based AAA service is disabled.

To enable the domain-based AAA service, run the **aaa domain enable** command.

Creating a Domain

By default, no domain is configured.

To configure a domain, run the **aaa domain** *domain-name* command.

Configuring an AV Set for a Domain

By default, no domain AV set is configured.

A domain AV set contains the following elements: AAA method lists, the maximum number of online users, whether to remove the domain name from the username, and whether the domain name takes effect.

Displaying Domain Configuration

To display domain configuration, run the **show aaa domain** command.

The system supports a maximum of 32 domains.

12.4 Configuration

Configuration	Description and Command	
Configuring AAA Authentication	Mandatory if user identities need to be verified.	
	aaa new-model	Enables AAA.
	aaa authentication login	Defines a method list of login authentication.
	aaa authentication enable	Defines a method list of Enable authentication.

12.4.1 Configuring AAA Authentication

Configuration Effect

Verify whether users are able to obtain access permission.

Notes

- If an authentication scheme contains multiple authentication methods, these methods are executed according to the configured sequence. The next authentication method is executed only when the current method does not respond. If the current method fails, the next method will be not tried.
- When the **none** method is used, users can get access even when no authentication method gets response. Therefore, the **none** method is used only as standby.

Normally, do not use None authentication. You can use the **none** method as the last optional authentication method in special cases. For example, all the users who may request access are trusted users and the users' work must not be delayed by system faults. Then you can use the **none** method to assign access permissions to these users when the authentication server does not respond. It is recommended that the local authentication method be added before the **none** method.

- If AAA authentication is enabled but no authentication method is configured and the default authentication method does not exist, users can directly log in to the Console without being authenticated. If users log in by other means, the users must pass local authentication.

- When a user enters the CLI after passing login authentication (the **none** method is not used), the username is recorded. When the user performs Enable authentication, the user is not prompted to enter the username again, because the username that the user entered during login authentication is automatically filled in. However, the user must enter the password previously used for login authentication.
- The username is not recorded if the user does not perform login authentication when entering the CLI or the **none** method is used during login authentication. Then, a user is required to enter the username each time when performing Enable authentication.

Configuration Steps

Enabling AAA

- Mandatory.
- Run the **aaa new-model** command to enable AAA.
- By default, AAA is disabled.

Defining a Method List of Login Authentication

- Run the **aaa authentication login** command to configure a method list of login authentication.
- This configuration is mandatory if you need to configure a login authentication method list (including the configuration of the default method list).
- By default, no method list of login authentication is configured.

Defining a Method List of Enable Authentication

- Run the **aaa authentication enable** command to configure a method list of Enable authentication.
- This configuration is mandatory if you need to configure an Enable authentication method list. (You can configure only the default method list.)
- By default, no method list of Enable authentication is configured.

Defining a Method List of PPP Authentication

- Run the **aaa authentication ppp** command to configure a method list of PPP authentication.
- This configuration is mandatory if you need to configure an authentication method list for PPP dial-up access.
- By default, no method list of PPP authentication is configured.

Defining a Method List of Web Authentication

- Run the **aaa authentication web-auth** command to configure a method list of Web authentication.
- This configuration is mandatory if you need to configure a Web authentication method list (including the configuration of the default method list).
- By default, no method list of Web authentication is configured.

Defining a Method List of iPortal Web Authentication

- Run the **aaa authentication iportal** command to configure a method list of iPortal Web authentication.
- This configuration is mandatory if you need to configure an iPortal Web authentication method list (including the configuration of the default method list).
- By default, no method list of iPortal Web authentication is configured.

Setting the Maximum Number of Login Attempts

- Optional.
- By default, a user is allowed to enter passwords up to three times during login.

Setting the Maximum Lockout Time After a Login Failure

- Optional.
- By default, a user is locked for 15 minutes after entering wrong passwords three times.

Enabling Local Account (username or subs) Sharing in Web and iPortal Authentication

- (Optional) This configuration is supported only on EG products. This function is supported by default on other types of FS products.
- By default, a local account cannot be shared among multiple STAs.

Verification

- Run the **show aaa method-list** command to display the configured method lists.
- Run the **show aaa lockout** command to display the settings of the maximum number of login attempts and the maximum lockout time after a login failure.
- Run the **show running-config** command to display the authentication method lists associated with login authentication and 802.1X authentication.

Related Commands

Enabling AAA

Command	aaa new-model
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	To enable the AAA services, run this command. None of the rest of AAA commands can be effective if AAA is not enabled.

Defining a Method List of Login Authentication

Command	**aaa authentication login** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default:** With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a login authentication method list in characters. *method*: Indicates authentication methods from **local**, **none**, **group**, and **subs**. A method list contains up to four methods. **local**: Indicates that the local user database is used for authentication. **none**: Indicates that authentication is not performed. **group**: Indicates that a server group is used for authentication. Currently, the RADIUS and TACACS+ server groups are supported. **subs**: Indicates that the subs database is used for authentication.
Command Mode	Global configuration mode
Usage Guide	If the AAA login authentication service is enabled on the NAS, users must perform login authentication negotiation through AAA. Run the **aaa authentication login** command to configure the default or optional method lists for login authentication. In a method list, the next method is executed only when the current method does not receive response. After you configure login authentication methods, apply the methods to the VTY lines that require login authentication; otherwise, the methods will not take effect.

Defining a Method List of Enable Authentication

Command	**aaa authentication enable default** *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of an Enable authentication method list in characters. *method*: Indicates authentication methods from **enable**, **local**, **none**, and **group**. A method list contains up to four methods. **enable**: Indicates that the password that is configured using the **enable** command is used for authentication. **local**: Indicates that the local user database is used for authentication. **none**: Indicates that authentication is not performed. **group**: Indicates that a server group is used for authentication. Currently, the RADIUS and TACACS+ server groups are supported.
Command Mode	Global configuration mode
Usage Guide	If the AAA login authentication service is enabled on the NAS, users must perform Enable authentication negotiation through AAA. Run the **aaa authentication enable** command to configure the default or optional method lists for Enable authentication. In a method list, the next method is executed only when the current method does not receive response.

Defining a Method List of PPP, Web, iPortal

Command	**aaa authentication** { **ppp | iportal** } { **default** | *list-name* } *method1* [*method2*...]

Parameter Description	**ppp:** Configures a method list of PPP authentication. **iportal**: Configures a method list of iportal authentication. **default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a PPP authentication method list in characters. *method*: Indicates authentication methods from **local**, **none**, **group**, and **subs**. A method list contains up to four methods. **local**: Indicates that the local user database is used for authentication. **none**: Indicates that authentication is not performed. **group**: Indicates that a server group is used for authentication. Currently, the RADIUS and TACACS+ server groups are supported. **subs**: Specifies the SUBS authentication method using the SUBS database.
Command Mode	Global configuration mode
Usage Guide	If the AAA PPP authentication service is enabled on the NAS, users must perform PPP authentication negotiation through AAA. Run the **aaa authentication ppp** command to configure the default or optional method lists for PPP authentication. In a method list, the next method is executed only when the current method does not receive response.

Setting the Maximum Number of Login Attempts

Command	**aaa local authentication attempts** *max-attempts*
Parameter Description	*max-attempts*: Indicates the maximum number of login attempts. The value ranges from 1 to 2,147,483,647.
Command Mode	Global configuration mode
Usage Guide	Use this command to set the maximum number of times a user can attempt to login.

Setting the Maximum Lockout Time After a Login Failure

Command	**aaa local authentication lockout-time** *lockout-time*
Parameter Description	*lockout-time*: Indicates the time during which a user is locked after entering wrong passwords up to the specified times. The value ranges from 1 to 2,147,483,647, in the unit of minutes.
Command Mode	Global configuration mode
Usage Guide	Use this command to set the maximum time during which a user is locked after entering wrong passwords up to the specified times.

Setting the Maximum Lockout Time After a Login Failure

Command	**aaa local user allow public account**
Parameter Description	N/A
Command Mode	Global configuration mode

Usage Guide	Use this command to configure local account (**username** or **subs**) sharing among multiple STAs in Web authentication or iPortal Web authentication.

Configuration Example

Configuring AAA Login Authentication

Configure a login authentication method list on the NAS containing **group** *radius* and **local** methods in order.

Scenario Figure 12-5	
Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS or TACACS+ server in advance if group-server authentication needs to be implemented. Configure the local user database information on the NAS if local authentication needs to be implemented. (This example requires the configuration of a RADIUS server and local database information.) Step 3: Configure an AAA authentication method list for login authentication users. (This example uses **group** *radius* and **local** in order.) Step 4: Apply the configured method list to an interface or line. Skip this step if the default authentication method is used.
NAS	FS#configure terminal FS(config)#username user password pass FS(config)#aaa new-model FS(config)#radius-server host 10.1.1.1 FS(config)#radius-server key FS FS(config)#aaa authentication login list1 group radius local FS(config)#line vty 0 20 FS(config-line)#login authentication list1 FS(config-line)#exit
Verification	Run the **show aaa method-list** command on the NAS to display the configuration.
NAS	FS#show aaa method-list Authentication method-list: aaa authentication login list1 group radius local Accounting method-list:

	Authorization method-list:
	Assume that a user remotely logs in to the NAS through Telnet. The user is prompted to enter the username and password on the CLI. The user must enter the correct username and password to access the NAS.
User	User Access Verification Username:user Password:pass

Configuring AAA Enable Authentication

Configure an Enable authentication method list on the NAS containing **group** *radius*, **local**, and then **enable** methods in order.

Scenario Figure 12-6	
Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS or TACACS+ server in advance if group-server authentication needs to be implemented. Configure the local user database information on the NAS if local authentication needs to be implemented. Configure Enable authentication passwords on the NAS if you use Enable password authentication. Step 3: Configure an AAA authentication method list for Enable authentication users. You can define only one Enable authentication method list globally. You do not need to define the list name but just default it. After that, it will be applied automatically.
NAS	FS#configure terminal FS(config)#username user privilege 15 password pass FS(config)#enable secret w FS(config)#aaa new-model FS(config)#radius-server host 10.1.1.1 FS(config)#radius-server key FS FS(config)#aaa authentication enable default group radius local enable
Verification	Run the **show aaa method-list** command on the NAS to display the configuration.
NAS	FS#show aaa method-list

	Authentication method-list: aaa authentication enable default group radius local enable Accounting method-list: Authorization method-list:
	The CLI displays an authentication prompt when the user level is updated to level 15. The user must enter the correct username and password to access the NAS.
NAS	FS>enable Username:user Password:pass FS#

Configuring AAA 802.1X Authentication

Configure an 802.1X authentication method list on the NAS containing **group** *radius*, and then **local** methods in order.

Scenario Figure 12-7	
Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS server in advance if group-server authentication needs to be implemented. Configure the local user database information on the NAS if local authentication needs to be implemented. (This example requires the configuration of a RADIUS server and local database information.) Currently, 802.1X authentication does not support TACACS+. Step 3: Configure an AAA authentication method list for 802.1X authentication users. (This example uses **group** *radius* and **local** in order.) Step 4: Apply the AAA authentication method list. Skip this step if the default authentication method is used. Step 5: Enable 802.1X authentication on an interface.
NAS	FS#configure terminal FS(config)#username user1 password pass1 FS(config)#username user2 password pass2 FS(config)#aaa new-model FS(config)#radius-server host 10.1.1.1 FS(config)#radius-server key FS

	FS(config)#aaa authentication dot1x default group radius local FS(config)#interface gigabitEthernet 0/1 FS(config-if-gigabitEthernet 0/1)#dot1 port-control auto FS(config-if-gigabitEthernet 0/1)#exit
Verification	Run the **show aaa method-list** command on the NAS to display the configuration.
NAS	FS#show aaa method-list Authentication method-list: aaa authentication dot1x default group radius local Accounting method-list: Authorization method-list:

Common Errors

- No RADIUS server or TACACS+ server is configured.
- Usernames and passwords are not configured in the local database.

12.4.2 Configuring AAA Authorization

Configuration Effect

- Determine what services or permissions authenticated users can enjoy.

Notes

- EXEC authorization is often used with login authentication, which can be implemented on the same line. Authorization and authentication can be performed using different methods and servers. Therefore, the results of the same user may be different. If a user passes login authentication but fails in EXEC authorization, the user cannot enter the CLI.
- The authorization methods in an authorization scheme are executed in accordance with the method configuration sequence. The next authorization method is executed only when the current method does not receive response. If authorization fails using a method, the next method will be not tried.
- Command authorization is supported only by TACACS+.
- Console authorization: The FSOS can differentiate between the users who log in through the Console and the users who log in through other types of clients. You can enable or disable command authorization for the users who log in through the Console. If command authorization is disabled for these users, the command authorization method list applied to the Console line no longer takes effect.

Configuration Steps

Enabling AAA

- Mandatory.
- Run the **aaa new-model** command to enable AAA.
- By default, AAA is disabled.

Defining a Method List of EXEC Authorization

- Run the **aaa authorization exec** command to configure a method list of EXEC authorization.
- This configuration is mandatory if you need to configure an EXEC authorization method list (including the configuration of the default method list).
- By default, no EXEC authorization method list is configured.

The default access permission level of EXEC users is the lowest. (Console users can connect to the NAS through the Console port or Telnet. Each connection is counted as an EXEC user, for example, a Telnet user and SSH user.)

Defining a Method List of Command Authorization

- Run the **aaa authorization commands** command to configure a method list of command authorization.
- This configuration is mandatory if you need to configure a command authorization method list (including the configuration of the default method list).
- By default, no command authorization method list is configured.

Configuring a Method List of Network Authorization

- Run the **aaa authorization network** command to configure a method list of network authorization.
- This configuration is mandatory if you need to configure a network authorization method list (including the configuration of the default method list).
- By default, no authorization method is configured.

Applying EXEC Authorization Methods to a Specified VTY Line

- Run the **authorization exec** command in line configuration mode to apply EXEC authorization methods to a specified VTY line.
- This configuration is mandatory if you need to apply an EXEC authorization method list to a specified VTY line.
- By default, all VTY lines are associated with the default authorization method list.

Applying Command Authorization Methods to a Specified VTY Line

- Run the **authorization commands** command in line configuration mode to apply command authorization methods to a specified VTY line.
- This configuration is mandatory if you need to apply a command authorization method list to a specified VTY line.
- By default, all VTY lines are associated with the default authorization method list.

Enabling Authorization for Commands in Configuration Modes

- Run the **aaa authorization config-commands** command to enable authorization for commands in configuration modes.
- By default, authorization is disabled for commands in configuration modes.

Enabling Authorization for the Console to Run Commands

- Run the **aaa authorization console** command to enable authorization for console users to run commands.
- By default, authorization is disabled for the Console to run commands.

Verification

Run the **show running-config** command to verify the configuration.

Related Commands

Enabling AAA

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	To enable the AAA services, run this command. None of the rest of AAA commands can be effective if AAA is not enabled.

Defining a Method List of EXEC Authorization

Command	**aaa authorization exec** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of an EXEC authorization method list in characters. *method*: Specifies authentication methods from **local**, **none**, and **group**. A method list contains up to four methods. **local**: Indicates that the local user database is used for EXEC authorization. **none**: Indicates that EXEC authorization is not performed. **group**: Indicates that a server group is used for EXEC authorization. Currently, the RADIUS and TACACS+ server groups are supported.
Command Mode	Global configuration mode
Usage Guide	The FSOS supports authorization of the users who log in to the CLI of the NAS to assign the users CLI operation permission levels (0 to 15). Currently, EXEC authorization is performed only on the users who have passed login authentication. If a user fails in EXEC authorization, the user cannot enter the CLI. After you configure EXEC authorization methods, apply the methods to the VTY lines that require EXEC authorization; otherwise, the methods will not take effect.

Defining a Method List of Command Authorization

Command	**aaa authorization commands** *level* { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a command authorization method list in characters. *method*: Indicates authentication methods from **none** and **group**. A method list contains up to four methods. **none**: Indicates that command authorization is not performed. **group**: Indicates that a server group is used for command authorization. Currently, the TACACS+ server group is supported.
Command Mode	Global configuration mode
Usage Guide	The FSOS supports authorization of the commands executable by users. When a user enters a command, AAA sends the command to the authentication server. If the authentication server permits the execution, the command is executed. If the authentication server forbids the execution, the command is not executed and a message is displayed showing that the execution is rejected. When you configure command authorization, specify the command level, which is used as the default level. (For example, if a command above Level 14 is visible to users, the default level of the command is 14.) After you configure command authorization methods, apply the methods to the VTY lines that require command authorization; otherwise, the methods will not take effect.

Configuring a Method List of Network Authorization

Command	**aaa authorization network** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a network authorization method list in characters. *method*: Indicates authentication methods from **none** and **group**. A method list contains up to four methods. **none**: Indicates that authentication is not performed. **group**: Indicates that a server group is used for network authorization. Currently, the RADIUS and TACACS+ server groups are supported.
Command Mode	Global configuration mode
Usage Guide	The FSOS supports authorization of network-related service requests such as PPP and SLIP requests. After authorization is configured, all authenticated users or interfaces are authorized automatically. You can configure three different authorization methods. The next authorization method is executed only when the current method does not receive response. If authorization fails using a method, the next method will be not tried. RADIUS or TACACS+ servers return a series of AV pairs to authorize authenticated users. Network authorization is based on authentication. Only authenticated users can perform network authorization.

Enabling Authorization for Commands in Configuration Modes (Including the Global Configuration Mode and Sub-Modes)

Command	**aaa authorization config-commands**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	If you need to enable authorization for commands only in non-configuration modes (for example, privileged EXEC mode), disable authorization in configuration modes by using the **no** form of this command. Then users can run commands in configuration mode and sub-modes without authorization.

Enabling Authorization for the Console to Run Commands

Command	**aaa authorization console**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	The FSOS can differentiate between the users who log in through the Console and the users who log in through other types of clients. You can enable or disable command authorization for the users who log in through the Console. If command authorization is disabled for these users, the command authorization method list applied to the Console line no longer takes effect.

Configuration Example

Configuring AAA EXEC Authorization

Configure login authentication and EXEC authorization for users on VTY lines 0 to 4. Login authentication is performed in local mode, and EXEC authorization is performed on a RADIUS server. If the RADIUS server does not respond, users are redirected to the local authorization.

Scenario **Figure 12-8**	
Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS or TACACS+ server in advance if remote server-group authorization needs to be implemented. If local authorization needs to be implemented, configure the local user database information on the NAS. Step 3: Configure an AAA authorization method list according to different access modes and service types. Step 4: Apply the configured method list to an interface or line. Skip this step if the default authorization method is used. EXEC authorization is often used with login authentication, which can be implemented on the

	same line.
NAS	FS#configure terminal FS(config)#username user password pass FS(config)#username user privilege 6 FS(config)#aaa new-model FS(config)#radius-server host 10.1.1.1 FS(config)#radius-server key test FS(config)#aaa authentication login list1 group local FS(config)#aaa authorization exec list2 group radius local FS(config)#line vty 0 4 FS(config-line)#login authentication list1 FS(config-line)# authorization exec list2 FS(config-line)#exit
Verification	Run the **show run** and **show aaa method-list** commands on the NAS to display the configuration.
NAS	FS#show aaa method-list Authentication method-list: aaa authentication login list1 group local Accounting method-list: Authorization method-list: aaa authorization exec list2 group radius local
	FS# show running-config aaa new-model ! aaa authorization exec list2 group local aaa authentication login list1 group radius local ! username user password pass username user privilege 6 ! radius-server host 10.1.1.1

	radius-server key 7 093b100133
	!
	line con 0
	line vty 0 4
	  authorization exec list2
	  login authentication list1
	!
	End

Configuring AAA Command Authorization

Provide command authorization for login users according to the following default authorization method: Authorize level-15 commands first by using a TACACS+ server. If the TACACS+ server does not respond, local authorization is performed. Authorization is applied to the users who log in through the Console and the users who log in through other types of clients.

Scenario Figure 12-9	
Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS or TACACS+ server in advance if remote server-group authorization needs to be implemented. If local authorization needs to be implemented, configure the local user database information on the NAS. Step 3: Configure an AAA authorization method list according to different access modes and service types. Step 4: Apply the configured method list to an interface or line. Skip this step if the default authorization method is used.
NAS	FS#configure terminal FS(config)#username user1 password pass1 FS(config)#username user1 privilege 15 FS(config)#aaa new-model FS(config)#tacacs-server host 192.168.217.10 FS(config)#tacacs-server key aaa FS(config)#aaa authentication login default local FS(config)#aaa authorization commands 15 default group tacacs+ local FS(config)#aaa authorization console
Verification	Run the **show run** and **show aaa method-list** commands on the NAS to display the configuration.
NAS	FS#show aaa method-list

```
Authentication method-list:
aaa authentication login default local

Accounting method-list:

Authorization method-list:
aaa authorization commands 15 default group tacacs+ local
```

```
FS#show run
!
aaa new-model
!
aaa authorization console
aaa authorization commands 15 default group tacacs+ local
aaa authentication login default local
!
!
nfpp
!
vlan 1
!
username user1 password 0 pass1
username user1 privilege 15
no service password-encryption
!
tacacs-server host 192.168.217.10
tacacs-server key aaa
!
line con 0
line vty 0 4
!
!
end
```

Configuring AAA Network Authorization

Scenario Figure 12-10	
Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS or TACACS+ server in advance if remote server-group authorization needs to be implemented. If local authorization needs to be implemented, configure the local user database information on the NAS. Step 3: Configure an AAA authorization method list according to different access modes and service types. Step 4: Apply the configured method list to an interface or line. Skip this step if the default authorization method is used.
NAS	FS#configure terminal FS(config)#aaa new-model FS(config)#radius-server host 10.1.1.1 FS(config)#radius-server key test FS(config)#aaa authorization network default group radius none FS(config)# end
Verification	Run the **show aaa method-list** command on the NAS to display the configuration.
NAS	FS#show aaa method-list Authentication method-list: Accounting method-list: Authorization method-list: aaa authorization network default group radius none

Common Errors

N/A

12.4.3 Configuring AAA Accounting

Configuration Effect

- Record the network resource usage of users.

- Record the user login and logout processes and the commands executed by users during device management.

Notes

About accounting methods:

- If an accounting scheme contains multiple accounting methods, these methods are executed according to the method configuration sequence. The next accounting method is executed only when the current method does not receive response. If accounting fails using a method, the next method will be not tried.
- After the default accounting method list is configured, it is applied to all VTY lines automatically. If a non-default accounting method list is applied to a line, it will replace the default one. If you apply an undefined method list to a line, the system will display a message indicating that accounting on this line is ineffective. Accounting will take effect only when a defined method list is applied.

EXEC accounting:

- EXEC accounting is performed only when login authentication on the NAS is completed. EXEC accounting is not performed if login authentication is not configured or the **none** method is used for authentication. If Start accounting is not performed for a user upon login, Stop accounting will not be performed when the user logs out.

Command accounting

- Only the TACACS+ protocol supports command accounting.

Configuration Steps

Enabling AAA

- Mandatory.
- Run the **aaa new-model** command to enable AAA.
- By default, AAA is disabled.

Defining a Method List of EXEC Accounting

- Run the **aaa accounting exec** command to configure a method list of EXEC accounting.
- This configuration is mandatory if you need to configure an EXEC accounting method list (including the configuration of the default method list).
- The default access permission level of EXEC users is the lowest. (Console users can connect to the NAS through the Console port or Telnet. Each connection is counted as an EXEC user, for example, a Telnet user and SSH user.)
- By default, no EXEC accounting method list is configured.

Defining a Method List of Command Accounting

- Run the **aaa accounting commands** command to configure a method list of command accounting.
- This configuration is mandatory if you need to configure a command accounting method list (including the configuration of the default method list).

- By default, no command accounting method list is configured. Only the TACACS+ protocol supports command accounting.

Defining a Method List of Network Accounting

- Run the **aaa accounting network** command to configure a method list of network accounting.
- This configuration is mandatory if you need to configure a network accounting method list (including the configuration of the default method list).
- By default, no network accounting method list is configured.

Applying EXEC Accounting Methods to a Specified VTY Line

- Run the **accounting exec** command in line configuration mode to apply EXEC accounting methods to a specified VTY line.
- This configuration is mandatory if you need to apply an EXEC accounting method list to a specified VTY line.
- You do not need to run this command if you apply the default method list.
- By default, all VTY lines are associated with the default accounting method list.

Applying Command Accounting Methods to a Specified VTY Line

- Run the **accounting commands** command in line configuration mode to apply command accounting methods to a specified VTY line.
- This configuration is mandatory if you need to apply a command accounting method list to a specified VTY line.
- You do not need to run this command if you apply the default method list.
- By default, all VTY lines are associated with the default accounting method list.

Enabling Accounting Update

- Optional.
- It is recommended that accounting update be configured for improved accounting accuracy.
- By default, accounting update is disabled.

Configuring the Accounting Update Interval

- Optional.
- It is recommended that the accounting update interval not be configured unless otherwise specified.

Verification

Run the **show running-config** command to verify the configuration.

Related Commands

Enabling AAA

Command	aaa new-model

Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	To enable the AAA services, run this command. None of the rest of AAA commands can be effective if AAA is not enabled.

Defining a Method List of EXEC Accounting

Command	**aaa accounting exec** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of an EXEC accounting method list in characters. *method*: Indicates authentication methods from **none** and **group**. A method list contains up to four methods. **none**: Indicates that EXEC accounting is not performed. **group**: Indicates that a server group is used for EXEC accounting. Currently, the RADIUS and TACACS+ server groups are supported.
Command Mode	Global configuration mode
Usage Guide	The FSOS enables EXEC accounting only when login authentication is completed. EXEC accounting is not performed if login authentication is not performed or the **none** authentication method is used. After accounting is enabled, when a user logs in to the CLI of the NAS, the NAS sends a start-accounting message to the authentication server. When the user logs out, the NAS sends a stop-accounting message to the authentication server. If the NAS does not send a start-accounting message when the user logs in, the NAS will not send a stop-accounting message when the user logs out. After you configure EXEC accounting methods, apply the methods to the VTY lines that require EXEC accounting; otherwise, the methods will not take effect.

Defining a Method List of Command Accounting

Command	**aaa accounting commands** *level* { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Parameter Description	*level*: Indicates the command level for which accounting will be performed. The value ranges from 0 to 15. After a command of the configured level is executed, the accounting server records related information based on the received accounting packet. **default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a command accounting method list in characters. *method*: Indicates authentication methods from **none** and **group**. A method list contains up to four methods. **none**: Indicates that command accounting is not performed. **group**: Indicates that a server group is used for command accounting. Currently, the TACACS+ server group is supported.
Command Mode	Global configuration mode
Usage Guide	The FSOS enables command accounting only when login authentication is completed. Command

	accounting is not performed if login authentication is not performed or the **none** authentication method is used. After accounting is enabled, the NAS records information about the commands of the configured level that users run and sends the information to the authentication server. After you configure command accounting methods, apply the methods to the VTY lines that require command accounting; otherwise, the methods will not take effect.

Defining a Method List of Network Accounting

Command	**aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a network accounting method list in characters. **start-stop**: Indicates that a start-accounting message and a stop-accounting message are sent when a user accesses a network and when the user disconnects from the network respectively. The start-accounting message indicates that the user is allowed to access the network, regardless of whether accounting is successfully enabled. *method*: Indicates authentication methods from **none** and **group**. A method list contains up to four methods. **none**: Indicates that network accounting is not performed. **group**: Indicates that a server group is used for network accounting. Currently, the RADIUS and TACACS+ server groups are supported.
Command Mode	Global configuration mode
Usage Guide	The FSOS sends record attributes to the authentication server to perform accounting of user activities. The **start-stop** keyword is used to configure user accounting options.

Enabling Accounting Update

Command	**aaa accounting update**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Accounting update cannot be used if the AAA services are not enabled. After the AAA services are enabled, run this command to enable accounting update.

Configuring the Accounting Update Interval

Command	**aaa accounting update periodic** *interval*
Parameter Description	*Interval*: Indicates the accounting update interval, in the unit of minutes. The shortest is 1 minute.
Command Mode	Global configuration mode
Usage Guide	Accounting update cannot be used if the AAA services are not enabled. After the AAA services are enabled, run this command to configure the accounting update interval.

Configuration Example

Configuring AAA EXEC Accounting

Configure login authentication and EXEC accounting for users on VTY lines 0 to 4. Login authentication is performed in local mode, and EXEC accounting is performed on a RADIUS server.

Scenario **Figure 12-11**	
Configuration Steps	Step 1: Enable AAA. If remote server-group accounting needs to be implemented, configure a RADIUS or TACACS+ server in advance. Step 2: Configure an AAA accounting method list according to different access modes and service types. Step 3: Apply the configured method list to an interface or line. Skip this step if the default accounting method is used.
NAS	FS#configure terminal FS(config)#username user password pass FS(config)#aaa new-model FS(config)#radius-server host 10.1.1.1 FS(config)#radius-server key test FS(config)#aaa authentication login list1 group local FS(config)#aaa accounting exec list3 start-stop group radius FS(config)#line vty 0 4 FS(config-line)#login authentication list1 FS(config-line)# accounting exec list3 FS(config-line)#exit
Verification	Run the **show run** and **show aaa method-list** commands on the NAS to display the configuration.
NAS	FS#show aaa method-list Authentication method-list: aaa authentication login list1 group local Accounting method-list: aaa accounting exec list3 start-stop group radius Authorization method-list:

```
FS# show running-config
aaa new-model
!
aaa accounting exec list3 start-stop group radius
aaa authentication login list1 group local
!
username user password   pass
!
radius-server host 10.1.1.1
radius-server key 7 093b100133
!
line con 0
line vty 0 4
 accounting   exec list3
 login authentication list1
!
End
```

Configuring AAA Command Accounting

Configure command accounting for login users according to the default accounting method. Login authentication is performed in local mode, and command accounting is performed on a TACACS+ server.

Scenario **Figure 12-12**	
Configuration Steps	Step 1: Enable AAA. If remote server-group accounting needs to be implemented, configure a RADIUS or TACACS+ server in advance. Step 2: Configure an AAA accounting method list according to different access modes and service types. Step 3: Apply the configured method list to an interface or line. Skip this step if the default accounting method is used.
NAS	FS#configure terminal FS(config)#username user1 password pass1 FS(config)#username user1 privilege 15

	FS(config)#aaa new-model FS(config)#tacacs-server host 192.168.217.10 FS(config)#tacacs-server key aaa FS(config)#aaa authentication login default local FS(config)#aaa accounting commands 15 default start-stop group tacacs+
Verification	Run the **show aaa method-list** command on the NAS to display the configuration.
NAS	FS#show aaa method-list Authentication method-list: aaa authentication login default local Accounting method-list: aaa accounting commands 15 default start-stop group tacacs+ Authorization method-list:
	FS#show run ! aaa new-model ! aaa authorization config-commands aaa accounting commands 15 default start-stop group tacacs+ aaa authentication login default local ! ! nfpp ! vlan 1 ! username user1 password 0 pass1 username user1 privilege 15 no service password-encryption ! tacacs-server host 192.168.217.10

```
tacacs-server key aaa
!
line con 0
line vty 0 4
!
!
end
```

Configuring AAA Network Accounting

Configure a network accounting method list for 802.1X STAs, and configure a RADIUS remote server for authentication and accounting.

Scenario Figure 12-13	
Configuration Steps	Step 1: Enable AAA. Step 2: If remote server-group accounting needs to be implemented, configure a RADIUS server in advance. Step 3: Configure an AAA accounting method list according to different access modes and service types. Step 4: Apply the configured AAA accounting method list. Skip this step if the default accounting method is used. Accounting is performed only when 802.1X authentication is completed.
NAS	FS#configure terminal FS(config)#username user password pass FS(config)#aaa new-model FS(config)#radius-server host 10.1.1.1 FS(config)#radius-server key test FS(config)#aaa authentication dot1x aut1x group radius local FS(config)#aaa accounting network acc1x start-stop group radius FS(config)#dot1x authentication aut1x FS(config)#dot1x accounting acc1x FS(config)#interface gigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)#dot1 port-control auto FS(config-if-GigabitEthernet 0/1)#exit

Verification	Run the **show aaa method-list** command on the NAS to display the configuration.
NAS	FS#show aaa method-list Authentication method-list: aaa authentication dot1x aut1x group radius local Accounting method-list: aaa accounting network acc1x start-stop group radius Authorization method-list:

Common Errors

N/A

12.4.4 Configuring an AAA Server Group

Configuration Effect

- Create a user-defined server group and add one or more servers to the group.
- When you configure authentication, authorization, and accounting method lists, name the methods after the server group name so that the servers in the group are used to handle authentication, authorization, and accounting requests.
- Use self-defined server groups to separate authentication, authorization, and accounting.

Notes

In a user-defined server group, you can specify and apply only the servers in the default server group.

Configuration Steps

Creating a User-Defined AAA Server Group

- Mandatory.
- Assign a meaningful name to the user-defined server group. Do not use the predefined **radius** and **tacacs+** keywords in naming.

Adding an AAA Server Group Member

- Mandatory.
- Run the **server** command to add AAA server group members.
- By default, a user-defined server group does not have servers.

Verification

Run the **show aaa group** command to verify the configuration.

Related Commands

Creating a User-Defined AAA Server Group

Command	**aaa group server** {**radius** | **tacacs+**} *name*
Parameter Description	*name*: Indicates the name of the server group to be created. The name must not contain the **radius** and **tacacs+** keywords because they are the names of the default RADIUS and TACACS+ server groups.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure an AAA server group. Currently, the RADIUS and TACACS+ server groups are supported.

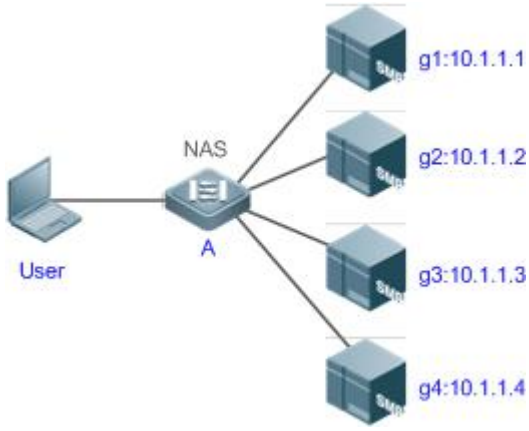
Adding an AAA Server Group Member

Command	**server** *ip-addr* [**auth-port** *port1*] [**acct-port** *port2*]
Parameter Description	*ip-addr*: Indicates the IP address of a server. *port1*: Indicates the authentication port of a server. (This parameter is supported only by the RADIUS server group.) *port2*: Indicates the accounting port of a server. (This parameter is supported only by the RADIUS server group.)
Command Mode	Server group configuration mode
Usage Guide	When you add servers to a server group, the default ports are used if you do not specify ports.

Configuration Example

Creating an AAA Server Group

Create RADIUS server groups named g1 and g2. The IP addresses of the servers in g1 are 10.1.1.1 and 10.1.1.2, and the IP addresses of the servers in g2 are 10.1.1.3 and 10.1.1.4.

Scenario Figure 12-14	
Prerequisites	1. The required interfaces, IP addresses, and VLANs have been configured on the network, network connections have been set up, and the routes from the NAS to servers are reachable. 2. Enable AAA.

Configuration Steps	Step 1: Configure a server (which belongs to the default server group). Step 2: Create user-defined AAA server groups. Step 3: Add servers to the AAA server groups.
NAS	FS#configure terminal FS(config)#radius-server host 10.1.1.1 FS(config)#radius-server host 10.1.1.2 FS(config)#radius-server host 10.1.1.3 FS(config)#radius-server host 10.1.1.4 FS(config)#radius-server key secret FS(config)#aaa group server radius g1 FS(config-gs-radius)#server 10.1.1.1 FS(config-gs-radius)#server 10.1.1.2 FS(config-gs-radius)#exit FS(config)#aaa group server radius g2 FS(config-gs-radius)#server 10.1.1.3 FS(config-gs-radius)#server 10.1.1.4 FS(config-gs-radius)#exit
Verification	Run the **show aaa group** and **show run** commands on the NAS to display the configuration.
NAS	FS#show aaa group Type Reference Name ---------- ---------- ---------- radius 1 radius tacacs+ 1 tacacs+ radius 1 g1 radius 1 g2
	FS#show run ! radius-server host 10.1.1.1 radius-server host 10.1.1.2 radius-server host 10.1.1.3 radius-server host 10.1.1.4 radius-server key secret !

```
aaa group server radius g1
 server 10.1.1.1
 server 10.1.1.2
!
aaa group server radius g2
 server 10.1.1.3
 server 10.1.1.4
!
!
```

Common Errors

- For RADIUS servers that use non-default authentication and accounting ports, when you run the **server** command to add servers, specify the authentication or accounting port.

12.4.5 Configuring the Domain-Based AAA Service

Configuration Effect

Create AAA schemes for 802.1X users in different domains.

Notes

About referencing method lists in domains:

- The AAA method lists that you select in domain configuration mode should be defined in advance. If the method lists are not defined in advance, when you select them in domain configuration mode, the system prompts that the configurations do not exist.
- The names of the AAA method lists selected in domain configuration mode must be consistent with those of the method lists defined for the AAA service. If they are inconsistent, the AAA service cannot be properly provided to the users in the domain.

About the default domain:

- Default domain: After the domain-based AAA service is enabled, if a username does not carry domain information, the AAA service is provided to the user based on the default domain. If the domain information carried by the username is not configured in the system, the system determines that the user is unauthorized and will not provide the AAA service to the user. If the default domain is not configured initially, it must be created manually.
- When the domain-based AAA service is enabled, the default domain is not configured by default and needs to be created manually. The default domain name is **default**. It is used to provide the AAA service to the users whose usernames do not carry domain information. If the default domain is not configured, the AAA service is not available for the users whose usernames do not carry domain information.

About domain names:

- The domain names carried by usernames and those configured on the NAS are matched in the longest matching principle. For example, if two domains, **domain.com** and **domain.com.cn** are configured on a NAS and a user sends a request carrying **aaa@domain.com**, the NAS determines that the user belongs to **domain.com**, instead of **domain.com.cn**.
- If the username of an authenticated user carries domain information but the domain is not configured on the NAS, the AAA service is not provided to the user.

Configuration Steps

Enabling AAA

- Mandatory.
- Run the **aaa new-model** command to enable AAA.
- By default, AAA is disabled.

Enabling the Domain-Based AAA Service

- Mandatory.
- Run the **aaa domain enable** command to enable the domain-based AAA service.
- By default, the domain-based AAA service is disabled.

Creating a Domain and Entering Domain Configuration Mode

- Mandatory.
- Run the **aaa domain** command to create a domain or enter the configured domain.
- By default, no domain is configured.

Associating the Domain with an 802.1X Authentication Method List

- Run the **authentication dot1x** command to associate the domain with an 802.1X authentication method list.
- This configuration is mandatory if you need to apply a specified 802.1X authentication method list to the domain.
- Currently, the domain-based AAA service is applicable only to 802.1X access.

Associating the Domain with a Network Accounting Method List

- Run the **accounting network** command to associate the domain with a network accounting method.
- This configuration is mandatory if you need to apply a specified network accounting method list to the domain.
- If a domain is not associated with a network accounting method list, by default, the global default method list is used for accounting.

Associating the Domain with a Network Authorization Method List

- Run the **authorization network** command to associate the domain with a network authorization method list.

- This configuration is mandatory if you need to apply a specified network authorization method list to the domain.
- If a domain is not associated with a network authorization method list, by default, the global default method list is used for authorization.

Configuring the Domain Status

- Optional.
- When a domain is in Block state, the users in the domain cannot log in.
- By default, after a domain is created, its state is Active, indicating that all the users in the domain are allowed to request network services.

Configuring Whether to Contain the Domain Name in Usernames

- Optional.
- By default, the usernames exchanged between the NAS and an authentication server carry domain information.

Configuring the Maximum Number of Domain Users

- Optional.
- By default, the maximum number of access users allowed in a domain is not limited.

Verification

Run the **show aaa domain** command to verify the configuration.

Related Commands

Enabling AAA

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	To enable the AAA services, run this command. None of the rest of AAA commands can be effective if AAA is not enabled.

Enabling the Domain-Based AAA Service

Command	**aaa domain enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to enable the domain-based AAA service.

Creating a Domain and Entering Domain Configuration Mode

Command	**aaa domain** { **default** | *domain-name* }
Parameter Description	**default**: Uses this parameter to configure the default domain. *domain-name*: Indicates the name of the domain to be created.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure a domain to provide the domain-based AAA service. The **default** parameter specifies the default domain. If a username does not carry domain information, the NAS uses the method list associated with the default domain to provide the AAA service to the user. The *domain-name* parameter specifies the name of the domain to be created. If the domain name carried by a username matches the configured domain name, the NAS uses the method list associated with this domain to provide the AAA service to the user. The system supports a maximum of 32 domains.

Associating the Domain with an 802.1X Authentication Method List

Command	**authentication dot1x** { **default** | *list-name* }
Parameter Description	**default**: Indicates that the default method list is used. *list-name*: Indicates the name of the method list to be associated.
Command Mode	Domain configuration mode
Usage Guide	Use this command to associate the domain with a 802.1X authentication method list.

Associating the Domain with a Web Authentication Method List

Command	**authentication web-auth** { **default** | *list-name* }
Parameter Description	**default**: Indicates that the default method list is used. *list-name*: Indicates the name of the method list to be associated.
Command Mode	Domain configuration mode
Usage Guide	Use this command to associate the domain with a Web authentication method list.

Associating the Domain with a Network Accounting Method List

Command	**accounting network** { **default** | *list-name* }
Parameter Description	**default**: Indicates that the default method list is used. *list-name*: Indicates the name of the method list to be associated.
Command Mode	Domain configuration mode
Usage Guide	Use this command to associate the domain with a network accounting method list.

Associating the Domain with a Network Authorization Method List

Command	**authorization network** { **default** | *list-name* }
Parameter Description	**default**: Indicates that the default method list is used. *list-name*: Indicates the name of the method list to be associated.
Command Mode	Domain configuration mode

Usage Guide	

Configuring the Domain Status

Command	**state** { **block** | **active** }
Parameter Description	**block**: Indicates that the configured domain is invalid. **active**: Indicates that the configured domain is valid.
Command Mode	Domain configuration mode
Usage Guide	Use this command to make the configured domain valid or invalid.

Configuring Whether to Contain the Domain Name in Usernames

Command	**username-format** { **without-domain** | **with-domain** }
Parameter Description	**without-domain**: Indicates to remove domain information from usernames. **with-domain**: Indicates to keep domain information in usernames.
Command Mode	Domain configuration mode
Usage Guide	Use this command in domain configuration mode to determine whether to include domain information in usernames when the NAS interacts with authentication servers in a specified domain.

Configuring the Maximum Number of Domain Users

Command	**access-limit** *num*
Parameter Description	*num*: Indicates the maximum number of access users allowed in a domain. This limit is applicable only to 802.1X STAs.
Command Mode	Domain configuration mode
Usage Guide	Use this command to limit the number of access users in a domain.

Configuration Example

Configuring the Domain-Based AAA Services

Configure authentication and accounting through a RADIUS server to 802.1X users (username: *user*@domain.com) that access the NAS. The usernames that the NAS sends to the RADIUS server do not carry domain information, and the number of access users is not limited.

Scenario **Figure 12-15**	
Configuration Steps	The following example shows how to configure RADIUS authentication and accounting, which requires the configuration of a RADIUS server in advance. Step 1: Enable AAA. Step 2: Define an AAA method list.

	Step 3: Enable the domain-based AAA service. Step 4: Create a domain. Step 5: Associate the domain with the AAA method list. Step 6: Configure the domain attribute.
NAS	FS#configure terminal FS(config)#aaa new-model FS(config)#radius-server host 10.1.1.1 FS(config)#radius-server key test FS(config)#aaa authentication dot1x default group radius FS(config)#aaa accounting network list3 start-stop group radius FS(config)# aaa domain enable FS(config)# aaa domain domain.com FS(config-aaa-domain)# authentication dot1x default FS(config-aaa-domain)# accounting network list3 FS(config-aaa-domain)# username-format without-domain
Verification	Run the **show run** and **show aaa domain** command on the NAS to display the configuration.

NAS	FS#show aaa domain domain.com
	
	==========Domain domain.com==========
	State: Active
	Username format: With-domain
	Access limit: No limit
	802.1X Access statistic: 0
	
	Selected method list:
	  authentication dot1x default
	  accounting network list3

	FS#show run Building configuration... Current configuration : 1449 bytes version FSOS 10.4(3) Release(101069)(Wed Oct 20 09:12:40 CST 2010 -ngcf67) co-operate enable

```
!
aaa new-model
aaa domain enable
!
aaa domain domain.com
 authentication dot1x default
 accounting network list3
!
aaa accounting network list3 start-stop group radius
aaa authentication dot1x default group radius
!
nfpp
!
no service password-encryption
!
radius-server host 10.1.1.1
radius-server key test
!
line con 0
line vty 0 4
!
end
```

Common Errors

N/A

12.5 Monitoring

Clearing

Description	Command
Clears the locked users.	**clear aaa local user lockout** {**all** | **user-name** *username* }

Displaying

Description	Command
Displays the accounting update information.	**show aaa accounting update**

Displays the current domain configuration.	**show aaa domain**
Displays the current lockout configuration.	**show aaa lockout**
Displays the AAA server groups.	**show aaa group**
Displays the AAA method lists.	**show aaa method-list**
Displays the AAA users.	**show aaa user**

13 Configuring RADIUS

13.1 Overview

The Remote Authentication Dial-In User Service (RADIUS) is a distributed client/server system.

RADIUS works with the Authentication, Authorization, and Accounting (AAA) to conduct identity authentication on users who attempt to access a network, to prevent unauthorized access. In FSOS implementation, a RADIUS client runs on a device or Network Access Server (NAS) and transmits identity authentication requests to the central RADIOUS server, where all user identity authentication information and network service information are stored. In addition to the authentication service, the RADIUS server provides authorization and accounting services for access users.

RADIUS is often applied in network environments that have high security requirements and allow the access of remote users. RADIUS is a completely open protocol and the RADIUS server is installed on many operating systems as a component, for example, on UNIX, Windows 2000, and Windows 2008. Therefore, RADIUS is the most widely applied security server currently.

The Dynamic Authorization Extensions to Remote Authentication Dial In User Service is defined in the IETF RFC3576. This protocol defines a user offline management method. Devices communicate with the RADIUS server through the Disconnect-Messages (DMs) to bring authenticated users offline. This protocol implements compatibility between devices of different vendors and the RADIUS server in terms of user offline processing.

In the DM mechanism, the RADIUS server actively initiates a user offline request to a device, the device locates a user according to the user session information, user name, and other information carried in the request and brings the user offline. Then, the device returns a response packet that carries the processing result to the RADIUS server, thereby implementing user offline management of the RADIUS server.

Protocols and Standards

- RFC2865: Remote Authentication Dial In User Service (RADIUS)
- RFC2866: RADIUS Accounting
- RFC2867: RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC2868: RADIUS Attributes for Tunnel Protocol Support
- RFC2869: RADIUS Extensions
- RFC3576: Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)

13.2 Applications

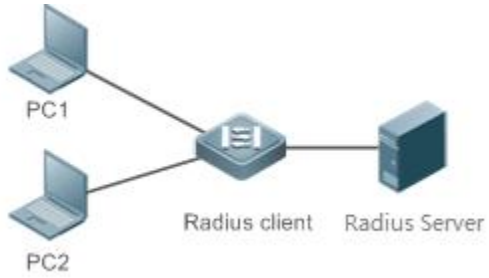
Application	Description
Providing Authentication, Authorization, and Accounting Services for Access Users	Authentication, authorization, and accounting are conducted on access users on a network, to prevent unauthorized access or operations.
Forcing Users to Go Offline	The server forces an authenticated user to go offline.

13.2.1 Providing Authentication, Authorization, and Accounting Services for Access Users

Scenario

RADIUS is typically applied in the authentication, authorization, and accounting of access users. A network device serves as a RADIUS client and transmits user information to a RADIUS server. After completing processing, the RADIUS server returns the authentication acceptance/authentication rejection/accounting response information to the RADIUS client. The RADIUS client performs processing on the access user according to the response from the RADIUS server.

Figure 13-1 Typical RADIUS Networking Topology



Remarks	PC 1 and PC 2 are connected to the RADIUS client as access users in wired or wireless mode, and initiate authentication and accounting requests. The RADIUS client is usually an access switch or aggregate switch. The RADIUS server can be a component built in the Windows 2000/2003, Server (IAS), or UNIX operating system or dedicated server software provided by vendors.

Deployment

- Configure access device information on the RADIUS server, including the IP address and shared key of the access devices.
- Configure the AAA method list on the RADIUS client.
- Configure the RADIUS server information on the RADIUS client, including the IP address and shared key.
- Enable access control on the access port of the RADIUS client.
- Configure the network so that the RADIUS client communicates with the RADIUS server successfully.

13.2.2 Forcing Users to Go Offline

Scenario

The RADIUS server forces authenticated online users to go offline for the sake of management.

See Figure 13-1 for the networking topology.

Deployment

- Add the following deployment on the basis of 1.2.1 "Deployment".
- Enable the RADIUS dynamic authorization extension function on the RADIUS client.

13.3 Features

Basic Concepts

Client/Server Mode

- Client: A RADIUS client initiates RADIUS requests and usually runs on a device or NAS. It transmits user information to the RADIUS server, receives responses from the RADIUS server, and performs processing accordingly. The processing includes accepting user access, rejecting user access, or collecting more user information for the RADIUS server.
- Server: Multiple RADIUS clients map to one RADIUS server. The RADIUS server maintains the IP addresses and shared keys of all RADIUS clients as well as information on all authenticated users. It receives requests from a RADIUS client, conducts authentication, authorization, and accounting, and returns processing information to the RADIUS client.

Structure of RADIUS Packets

The following figure shows the structure of RADIUS packets.

8	16	32bit
Code	Identifier	Length
Authenticator (16bytes)		
Attributes		

- Code: Identifies the type of RADIUS packets, which occupies one byte. The following table lists the values and meanings.

Code	Packet Type	Code	Packet Type
1	Access-Request	4	Accounting-Request
2	Access-Accept	5	Accounting-Response
3	Access-Reject	11	Access-Challenge

- Identifier: Indicates the identifier for matching request packets and response packets, which occupies one byte. The identifier values of request packets and response packets of the same type are the same.
- Length: Identifies the length of a whole RADIUS packet, which includes **Code**, **Identifier**, **Length**, **Authenticator**, and **Attributes**. It occupies two bytes. Bytes that are beyond the **Length** field will be truncated. If the length of a received packet is smaller than the value of **Length**, the packet is discarded.
- Authenticator: Verifies response packets of the RADIUS server by a RADIUS client, which occupies 16 bytes. This field is also used for encryption/decryption of user passwords.
- Attributes: Carries authentication, authorization, and accounting information, with the length unfixed. The **Attributes** field usually contains multiple attributes. Each attribute is represented in the Type,

Length, Value (TLV) format. Type occupies one byte and indicates the attribute type. The following table lists common attributes of RADIUS authentication, authorization, and accounting. Length occupies one byte and indicates the attribute length, with the unit of bytes. Value indicates the attribute information.

Attribute No.	Attribute Name	Attribute No.	Attribute Name
1	User-Name	43	Acct-Output-Octets
2	User-Password	44	Acct-Session-Id
3	CHAP-Password	45	Acct-Authentic
4	NAS-IP-Address	46	Acct-Session-Time
5	NAS-Port	47	Acct-Input-Packets
6	Service-Type	48	Acct-Output-Packets
7	Framed-Protocol	49	Acct-Terminate-Cause
8	Framed-IP-Address	50	Acct-Multi-Session-Id
9	Framed-IP-Netmask	51	Acct-Link-Count
10	Framed-Routing	52	Acct-Input-Gigawords
11	Filter-ID	53	Acct-Output-Gigawords
12	Framed-MTU	55	Event-Timestamp
13	Framed-Compression	60	CHAP-Challenge
14	Login-IP-Host	61	NAS-Port-Type
15	Login-Service	62	Port-Limit
16	Login-TCP-Port	63	Login-LAT-Port
18	Reply-Message	64	Tunnel-Type
19	Callback-Number	65	Tunnel-Medium-Type
20	Callback-ID	66	Tunnel-Client-Endpoint
22	Framed-Route	67	Tunnel-Server-Endpoint
23	Framed-IPX-Network	68	Acct-Tunnel-Connection
24	State	69	Tunnel-Password
25	Class	70	ARAP-Password
26	Vendor-Specific	71	ARAP-Features
27	Session-Timeout	72	ARAP-Zone-Access
28	Idle-Timeout	73	ARAP-Security
29	Termination-Action	74	ARAP-Security-Data
30	Called-Station-Id	75	Password-Retry
31	Calling-Station-Id	76	Prompt
32	NAS-Identifier	77	Connect-Info
33	Proxy-State	78	Configuration-Token
34	Login-LAT-Service	79	EAP-Message
35	Login-LAT-Node	80	Message-Authenticator
36	Login-LAT-Group	81	Tunnel-Private-Group-id
37	Framed-AppleTalk-Link	82	Tunnel-Assignment-id
38	Framed-AppleTalk-Network	83	Tunnel-Preference
39	Framed-AppleTalk-Zone	84	ARAP-Challenge-Respons

Attribute No.	Attribute Name	Attribute No.	Attribute Name
			e
40	Acct-Status-Type	85	Acct-Interim-Interval
41	Acct-Delay-Time	86	Acct-Tunnel-Packets-Los t
42	Acct-Input-Octets	87	NAS-Port-Id

Shared Key

A RADIUS client and a RADIUS server mutually confirm their identities by using a shared key during communication. The shared key cannot be transmitted over a network. In addition, user passwords are encrypted for transmission for the sake of security.

RADIUS Server Group

The RADIUS security protocol, also called RADIUS method, is configured in the form of a RADIUS server group. Each RADIUS method corresponds to one RADIUS server group and one or more RADIUS severs can be added to one RADIUS server group. For details about the RADIUS method, see the *Configuring AAA*. If you add multiple RADIUS servers to one RADIUS server group, when the communication between a device and the first RADIUS server in this group fails or the first RADIUS server becomes unreachable, the device automatically attempts to communicate with the next RADIUS server till the communication is successful or the communication with all the RADIUS servers fails.

RADIUS Attribute Type

- Standard attributes

The RFC standards specify the RADIUS attribute numbers and attribute content but do not specify the format of some attribute types. Therefore, the format of attribute contents needs to be configured to adapt to different RADIUS server requirements. Currently, the format of the RADIUS Calling-Station-ID attribute (attribute No.: 31) can be configured.

The RADIUS Calling-Station-ID attribute is used to identify user identities when a network device transmits request packets to the RADIUS server. The RADIUS Calling-Station-ID attribute is a string, which can adopt multiple formats. It needs to uniquely identify a user. Therefore, it is often set to the MAC address of a user. For example, when IEEE 802.1X authentication is used, the Calling-Station-ID attribute is set to the MAC address of the device where the IEEE 802.1X client is installed. The following table describes the format of MAC addresses.

Format	Description
Ietf	Indicates the standard format specified in the IETF standard (RFC3580), which is separated by the separator (-). Example: 00-D0-F8-33-22-AC
Normal	Indicates the common format that represents a MAC address (dotted hexadecimal format), which is separated by the separator (.). Example: 00d0.f833.22ac
Unformatted	Indicates the format without separators. This format is used by default. Example: 00d0f83322ac

- Private attributes

RADIUS is an extensible protocol. According to RFC2865, the Vendor-Specific attribute (attribute No.: 26) is used by device vendors to extend the RADIUS protocol to implement private functions or functions that are not defined in the standard RADIUS protocol. Table 1-3 lists private attributes supported by FS products. The **TYPE** column indicates the default configuration of private attributes of FS products and the **Extended TYPE** column indicates the default configuration of private attributes of other non-FS products.

ID	Function	TYPE	Extended TYPE
1	max-down-rate	1	76
2	port-priority	2	77
3	user-ip	3	3
4	vlan-id	4	4
5	last-supplicant-version	5	5
6	net-ip	6	6
7	user-name	7	7
8	password	8	8
9	file-directory	9	9
10	file-count	10	10
11	file-name-0	11	11
12	file-name-1	12	12
13	file-name-2	13	13
14	file-name-3	14	14
15	file-name-4	15	15
16	max-up-rate	16	16
17	current-supplicant-version	17	17
18	flux-max-high32	18	18
19	flux-max-low32	19	19
20	proxy-avoid	20	20
21	dailup-avoid	21	21
22	ip-privilege	22	22
23	login-privilege	42	42
27	ipv4-multicast-address	87	87
62	sdg-type	62	62
85	sdg-zone-name	85	85
103	sdg-group-name	103	103

Overview

Feature	Description
RADIUS Authentication, Authorization, and Accounting	Conducts identity authentication and accounting on access users, safeguards network security, and facilitates management for network administrators.
Source Address of RADIUS Packets	Specifies the source IP address used by a RADIUS client to transmit packets to a RADIUS server.

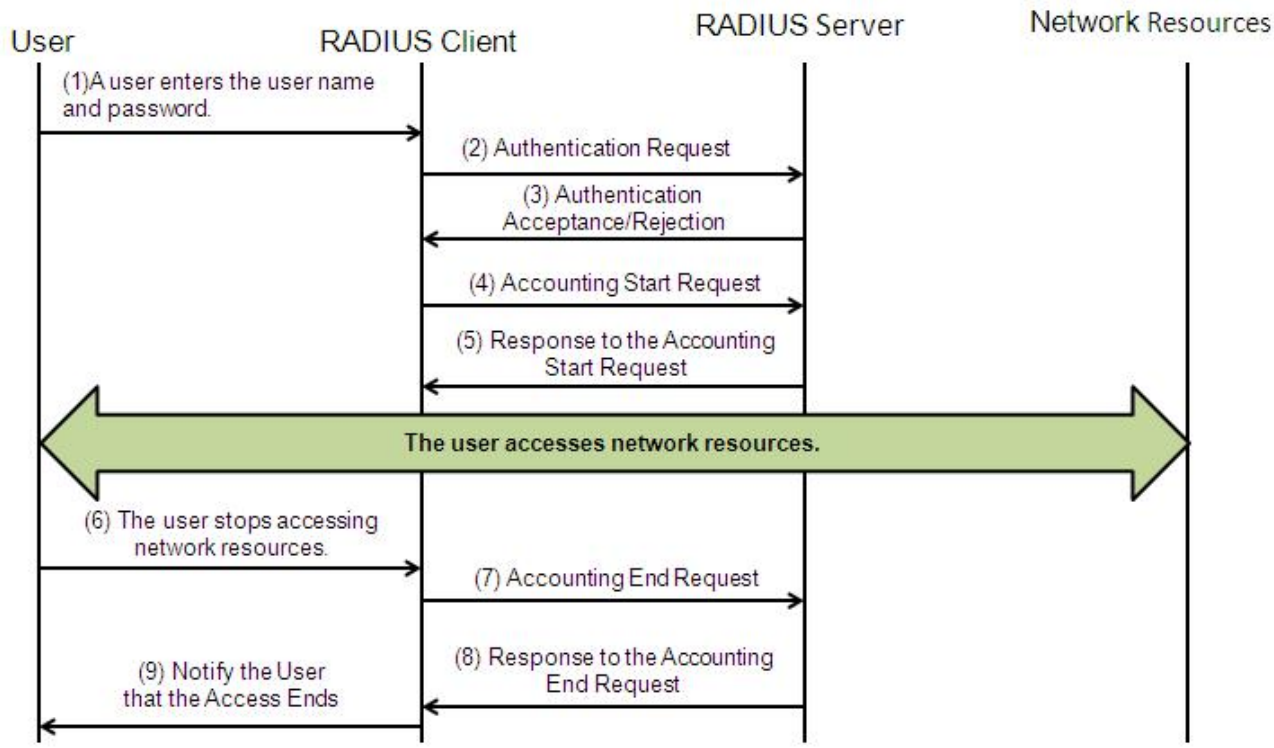
RADIUS Timeout Retransmission	Specifies the packet retransmission parameter for a RADIUS client when a RADIUS server does not respond to packets transmitted from the RADIUS client within a period of time.
RADIUS Server Accessibility Detection	Enables a RADIUS client to actively detect whether a RADIUS server is reachable and maintain the accessibility of each RADIUS server. A reachable RADIUS server is selected preferentially to improve the handling performance of RADIUS services.
RADIUS Forced Offline	Enables a RADIUS server to actively force authenticated users to go offline.

13.3.1 RADIUS Authentication, Authorization, and Accounting

Conduct identity authentication and accounting on access users, safeguard network security, and facilitate management for network administrators.

Working Principle

Figure 13-2



The RADIUS authentication and authorization process is described as follows:

1. A user enters the user name and password and transmits them to the RADIUS client.
2. After receiving the user name and password, the RADIUS client transmits an authentication request packet to the RADIUS server. The password is encrypted for transmission. For the encryption method, see RFC2865.

3. The RADIUS server accepts or rejects the authentication request according to the user name and password. When accepting the authentication request, the RADIUS server also issues authorization information apart from the authentication acceptance information. The authorization information varies with the type of access users.

The RADIUS accounting process is described as follows:

1. If the RADIUS server returns authentication acceptance information in Step (3), the RADIUS client sends an accounting start request packet to the RADIUS server immediately.
2. The RADIUS server returns the accounting start response packet, indicating accounting start.
3. The user stops accessing network resources and requests the RADIUS client to disconnect the network connection.
4. The RADIUS client transmits the accounting end request packet to the RADIUS server.
5. The RADIUS server returns the accounting end response packet, indicating accounting end.
6. The user is disconnected and cannot access network resources.

Related Configuration

Configuring RADIUS Server Parameters

No RADIUS server is configured by default.

You can run the **radius-server host** command to configure a RADIUS server.

At least one RADIUS server must be configured so that RADIUS services run normally.

Configuring the AAA Authentication Method List

No AAA authentication method list is configured by default.

You can run the **aaa authentication** command to configure a method list for different user types and select **group radius** when setting the authentication method.

The RADIUS authentication can be conducted only after the AAA authentication method list of relevant user types is configured.

Configuring the AAA Authorization Method List

No AAA authorization method list is configured by default.

You can run the **aaa authorization** command to configure an authorization method list for different user types and select **group radius** when setting the authorization method.

The RADIUS authorization can be conducted only after the AAA authorization method list of relevant user types is configured.

Configuring the AAA Accounting Method List

No AAA accounting method list is configured by default.

You can run the **aaa accounting** command to configure an accounting method list for different user types and select **group radius** when setting the accounting method.

The RADIUS accounting can be conducted only after the AAA accounting method list of relevant user types is configured.

13.3.2 Source Address of RADIUS Packets

Specify the source IP address used by a RADIUS client to transmit packets to a RADIUS server.

Working Principle

When configuring RADIUS, specify the source IP address to be used by a RADIUS client to transmit RADIUS packets to a RADIUS server, in an effort to reduce the workload of maintaining a large amount of NAS information on the RADIUS server.

Related Configuration

The global routing is used to determine the source address for transmitting RADIUS packets by default.

Run the **ip radius source-interface** command to specify the source interface for transmitting RADIUS packets. The device uses the first IP address of the specified interface as the source address of RADIUS packets.

13.3.3 RADIUS Timeout Retransmission

Working Principle

After a RADIUS client transmits a packet to a RADIUS server, a timer is started to detect the response of the RADIUS server. If the RADIUS server does not respond within a certain period of time, the RADIUS client retransmits the packet.

Related Configuration

↘ Configuring the RADIUS Server Timeout Time

The default timeout time is 5 seconds.

You can run the **radius-server timeout** command to configure the timeout time. The value ranges from 1 second to 1,000 seconds.

The response time of a RADIUS server is relevant to its performance and the network environment. Set an appropriate timeout time according to actual conditions.

↘ Configuring the Retransmission Count

The default retransmission count is 3.

You can run the **radius-server retransmit** command to configure the retransmission count. The value ranges from 1 to 100.

↘ Configuring Whether to Retransmit Accounting Update Packets

Accounting update packets are not retransmitted by default.

You can run the **radius-server account update retransmit** command to configure retransmission of accounting update packets for authenticated users.

13.3.4 RADIUS Server Accessibility Detection

Working Principle

A RADIUS client actively detects whether a RADIUS server is reachable and maintains the accessibility of each RADIUS server. A reachable RADIUS server is selected preferentially to improve the handling performance of RADIUS services.

Related Configuration

Configuring the Criteria for the Device to Judge That a RADIUS Server Is Unreachable

The default criteria configured for judging that a RADIUS server is unreachable meet the two conditions simultaneously: 1. The device does not receive a correct response packet from the RADIUS security server within 60 seconds. 2. The device transmits the request packet to the same RADIUS security server for consecutive 10 times.

You can run the **radius-server dead-criteria** command to configure the criteria for the device to judge that the RADIUS security server is unreachable.

Configuring the Test User Name for Actively Detecting the RADIUS Security Server

No test user name is specified for actively detecting the RADIUS security server by default.

You can run the **radius-server host x.x.x.xtestusername xxx** command to configure the test user name.

13.3.5 RADIUS Forced Offline

Working Principle

Figure 13-3 DM Message Exchange of the RADIUS Dynamic Authorization Extension Protocol

The preceding figure shows the exchange of DM messages between the RADIUS server and the device. The RADIUS server transmits the Disconnect-Request message to UDP Port 3799 of the device. After processing, the device returns the Disconnect-Response message that carries the processing result to the RADIUS server.

Related Configuration

N/A

13.4 Configuration

Configuration	Description and Command
RADIUS Basic Configuration	(Mandatory) It is used to configure RADIUS authentication, authorization, and accounting.

Configuration	Description and Command	
	radius-serverhost	Configures the IP address of the remote RADIUS security server.
	radius-serverkey	Configures the shared key for communication between the device and the RADIUS server.
	radius-serverretransmit	Configures the request transmission count, after which the device confirms that a RADIUS server is unreachable.
	radius-servertimeout	Configures the waiting time, after which the device retransmits a request.
	radius-server account update retransmit	Configures retransmission of accounting update packets for authenticated users.
	ip radius source-interface	Configures the source address of RADIUS packets.
Configuring the RADIUS Attribute Type	(Optional) It is used to define attribute processing adopted when the device encapsulates and parses RADIUS packets.	
	radius-serverattribute31	Configures the MAC address format of RADIUS attribute No. 31 (Calling-Station-ID).
	radius-server attribute class	Configures the parsing mode of the RADIUS Class attribute.
	radius attribute	Configures the RADIUS private attribute type.
	radius set qoscos	Sets the private attribute port-priority issued by the server to the COS value of an interface. For COS-relevant concepts, see the *Configuring QoS*.
	radius support cui	Configures the device to support the CUI attribute.
	radius vendor-specific	Configures the mode of parsing private attributes by the device.
	radius-server authentication attribute	Configures whether RADIUS authentication request packets carry a specified attribute.
	radius-server account attribute	Configures whether RADIUS accounting request packets carry a specified attribute.
	radius-server authentication vendor	Configures whether RADIUS authentication request packets carry the private attributes of other vendors.
	radius-server account vendor	Configures whether RADIUS accounting request packets carry the private attributes of other vendors.
Configuring RADIUS Accessibility Detection	(Optional) It is used to detect whether a RADIUS server is reachable and maintain the accessibility of the RADIUS server.	
	radius-server dead-criteria	Configures the global criteria for judging that a RADIUS security server is unreachable.

Configuration	Description and Command	
	radius-server deadtime	Configures the duration for the device to stop transmitting request packets to an unreachable RADIUS server.
	radius-server host	Configures the IP address of the remote RADIUS security server, authentication port, accounting port, and active detection parameters.

13.4.1 RADIUS Basic Configuration

Configuration Effect

- RADIUS authentication, authorization, and accounting can be conducted after RADIUS basic configuration is complete.

Notes

- Before configuring RADIUS on the device, ensure that the network communication of the RADIUS server is in good condition.
- When running the **ip radius source-interface** command to configure the source address of RADIUS packets, ensure that the device of the source IP address communicates with the RADIUS server successfully.

Configuration Steps

Configuring the Remote RADIUS Security Server

- Mandatory.
- Configure the IP address, authentication port, accounting port, and shard key of the RADIUS security server.

Configuring the Shared Key for Communication Between the Device and the RADIUS Server

- Optional.
- Configure a shared key in global configuration mode for servers without a shared key.

The shared key on the device must be consistent with that on the RADIUS server.

Configuring the Request Transmission Count, After Which the Device Confirms That a RADIUS Server Is Unreachable

- Optional.
- Configure the request transmission count, after which the device confirms that a RADIUS server is unreachable, according to the actual network environment.

Configuring the Waiting Time, After which the Device Retransmits a Request

- Optional.

- Configure the waiting time, after which the device retransmits a request, according to the actual network environment.

In an 802.1X authentication environment that uses the RADIUS security protocol, if a network device serves as the 802.1X authenticator and FS SU is used as the 802.1X client software, it is recommended that **radius-server timeout** be set to 3 seconds (the default value is 5 seconds) and **radius-server retransmit** be set to 2 (the default value is 3) on the network device.

Configuring Retransmission of Accounting Update Packets for Authenticated Users

- Optional.
- Determine whether to enable the function of retransmitting accounting update packets of authenticated users according to actual requirements.

Configuring the Source Address of RADIUS Packets

- Optional.
- Configure the source address of RADIUS packets according to the actual network environment.

Verification

- Configure the AAA method list that specifies to conduct authentication, authorization, and accounting on users by using RADIUS.
- Enable the device to interact with the RADIUS server. Conduct packet capture to confirm that the device communicates with the RADIUS server over the RADIUS protocol.

Related Commands

Configuring the Remote RADIUS Security Server

Command	**radius-server host** [**oob**] { *ipv4-address* } [**auth-port** *port-number*] [**acct-port** *port-number*] [**test username** *name* [**idle-time** *time*] [**ignore-auth-port**] [**ignore-acct-port**]] [**key** [**0** | **7**] *text-string*]
Parameter Description	**oob**: Indicates oob authentication, that is, the source interface for transmitting packets to the RADIUS server is an mgmt port. *ipv4-address*: Indicates the IPv4 address of the RADIUS security server. **auth-port***port-number*: Indicates the UDP port for RADIUS identity authentication. The value ranges from 0 to 65,535. If it is set to **0**, the host does not conduct identity authentication. **acct-port** *port-number*: Indicates the UDP port for RADIUS accounting. The value ranges from 0 to 65,535. If it is set to **0**, the host does not conduct accounting. **test username** *name*: Enables the function of actively detecting the RADIUS security server and specifies the user name used for active detection. **idle-time***time*: Indicates the interval for the device to transmit test packets to a reachable RADIUS security server. The default value is 60 minutes. The value ranges from 1 minute to 1,440 minutes (24 hours). **ignore-auth-port**: Disables the function of detecting the authentication port of the RADIUS security server. It is enabled by default. **ignore-acct-port**: Disables the function of detecting the accounting port of the RADIUS security

	server. It is enabled by default. **key**[**0** | **7**] *text-string* : Configures the shared key of the server. The global shared key is used if it is not configured. The configured key is displayed as "*" and you are required to enter the same key twice. If the entered keys are inconsistent, you need to re-enter the key. If inconsistency occurs for five consecutive times, the configuration will fail.
Command Mode	Global configuration mode
Usage Guide	A RADIUS security server must be defined to implement the AAA security service by using RADIUS. You can run the **radius-server host** command to define one or more RADIUS security servers. If a RADIUS security server is not added to a RADIUS server group, the device uses the global routing table when transmitting RADIUS packets to the RADIUS server.

Configuring the Shared Key for Communication Between the Device and the RADIUS Server

Command	**radius-server key** [**0** | **7**]*text-string*
Parameter Description	*text-string*: Indicates the text of the shared key. **0 | 7**: Indicates the encryption type of the key. The value **0** indicates no encryption and **7**indicates simple encryption. The default value is **0**.
Command Mode	Global configuration mode
Usage Guide	A shared key is the basis for correct communication between the device and the RADIUS security server. The same shared key must be configured on the device and RADIUS security server so that they can communicate with each other successfully.

Configuring the Request Transmission Count, After Which the Device Confirms That a RADIUS Server Is Unreachable

Command	**radius-server retransmit***retries*
Parameter Description	*retries*: Indicates the RADIUS retransmission count. The value ranges from 1 to 100.
Command Mode	Global configuration mode
Usage Guide	The prerequisite for AAA to use the next user authentication method is that the current security server used for authentication does not respond. The criteria for the device to judge that a security server does not respond are that the security server does not respond within the RADIUS packet retransmission duration of the specified retransmission count. There is an interval between consecutive two retransmissions.

Configuring the Waiting Time, After which the Device Retransmits a Request

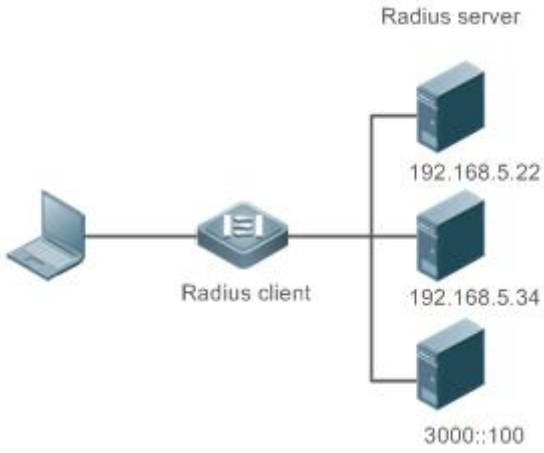
Command	**radius-server timeout***seconds*
Parameter Description	*seconds*: Indicates the timeout time, with the unit of seconds. The value ranges from 1 second to 1,000 seconds.
Command Mode	Global configuration mode
Usage Guide	Use this command to adjust the packet retransmission timeout time.

Configuring Retransmission of Accounting Update Packets for Authenticated Users

Command	**radius-server account update retransmit**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure retransmission of accounting update packets for authenticated users. Accounting update packets are not retransmitted by default. The configuration does not affect users of other types.

Configuration Example

Using RADIUS Authentication, Authorization, and Accounting for Login Users

Scenario Figure 13-4	
Configuration Steps	● Enable AAA. ● Configure the RADIUS server information. ● Configure to use the RADIUS authentication, authorization, and accounting methods. ● Apply the configured authentication method on the interface.
RADIUS Client	FS#configure terminal FS (config)#aaa new-model FS (config)# radius-server host 192.168.5.22 FS (config)#radius-server host 3000::100 FS (config)# radius-server key aaa FS (config)#aaa authentication login test group radius FS (config)#aaa authorizationexectest group radius FS (config)#aaa accountingexectest start-stop group radius FS (config)# line vty 0 4 FS (config-line)#login authentication test FS (config-line)# authorization exec test

	FS (config-line)# accounting exec test
Verification	Telnet to a device from a PC. The screen requesting the user name and password is displayed. Enter the correct user name and password to log in to the device. After obtaining a certain access level granted by the server, only run commands under this access level. Display the authentication log of the user on the RADIUS server. Perform management operations on the device as the user and then log out. Display the accounting information on the user on the RADIUS server.
	FS#show running-config ! radius-server host 192.168.5.22 radius-server host 3000::100 radius-server key aaa aaa new-model aaa accounting exec test start-stop group radius aaa authorization exec test group radius aaa authentication login test group radius no service password-encryption iptcp not-send-rst ! vlan 1 ! line con 0 line vty 0 4 accounting exec test authorization exec test login authentication test !

Common Errors

- The key configured on the device is inconsistent with that configured on the server.
- No method list is configured.

13.4.2 Configuring the RADIUS Attribute Type

Configuration Effect

- Define the attribute processing adopted when the device encapsulates and parses RADIUS packets.

Notes

- Private attributes involved in "Configuring the RADIUS Attribute Type" refer to FS private attributes.

Configuration Steps

Configuring the MAC Address Format of RADIUS Attribute No. 31 (Calling-Station-ID)

- Optional.
- Set the MAC address format of **Calling-Station-Id** to a type supported by the server.

Configuring the Parsing Mode of the RADIUS Class Attribute

- Optional.
- Configure the parsing mode of the Class attribute according to the server type.

Configuring the RADIUS Private Attribute Type

- Optional.
- If the server is a FS application server, the RADIUS private attribute type needs to be configured.

Setting the Private Attribute port-priority Issued by the Server to the COS Value of an Interface

- Optional.
- Set the private attribute **port-priority** issued by the server to the COS value of an interface as required.

Configures the Device to Support the CUI Attribute

- Optional.
- Configure whether the device supports the RADIUS CUI attribute as required.

Configuring the Mode of Parsing Private Attributes by the Device

- Optional.
- Configure the index of a FS private attribute parsed by the device as required.

Configuring Whether RADIUS Authentication Request Packets Carry a Specified Attribute

- Optional.
- Configure whether to specify the attribute type for RADIUS authentication request packets as required.

Configuring Whether RADIUS Accounting Request Packets Carry a Specified Attribute

- Optional.
- Configure whether to specify the attribute type for RADIUS accounting request packets as required.

Configuring Whether RADIUS Authentication Request Packets Carry the Private Attribute of a Specified Vendor

- Optional.

- Configure whether RADIUS authentication request packets carry the private attribute of a specified vendor as required.

Configuring Whether RADIUS Accounting Request Packets Carry the Private Attribute of a Specified Vendor

- Optional.
- Configure whether RADIUS accounting request packets carry the private attribute of a specified vendor as required.

Configuring Whether RADIUS Server Parses the Private Attribute of Cisco, Huawei or Microsoft

- Optional.
- Configure whether RADIUS server parses the private attribute of Cisco, Huawei or Microsoft.

Configuring the Nas-Port-Id Encapsulation Format for RADIUS Packets

- Optional.
- In either QINQ or non-QINQ scenarios, configure the nas-nort-id encapsulation format for RADIUS packets. By default, the packets are encapsulated in the normal format.

Verification

- Configure the AAA method list that specifies to conduct authentication, authorization, and accounting on users by using RADIUS.
- Enable the device to interact with the RADIUS server. Conduct packet capture to display the MAC address format of Calling-Station-Id.
- Enable the device to interact with the RADIUS server. Display the debug information of the device to check that FS private attributes are correctly parsed by the device.
- Enable the device to interact with the RADIUS server. Display the debug information of the device to check that the CUI attribute is correctly parsed by the device.

Related Commands

Configuring the MAC Address Format of RADIUS Attribute No. 31 (Calling-Station-ID)

Command	**radius-server attribute 31 mac format** {**ietf** | **normal** | **unformatted** }
Parameter Description	**ietf**: Indicates the standard format specified in the IETF standard (RFC3580), which is separated by the separator (-). Example: 00-D0-F8-33-22-AC. normal: Indicates the common format that represents a MAC address (dotted hexadecimal format), which is separated by the separator (.). Example: 00d0.f833.22ac. **unformatted**: Indicates the format without separators. This format is used by default. Example: 00d0f83322ac.
Command Mode	Global configuration mode
Usage Guide	Some RADIUS security servers (mainly used for 802.1X authentication) can identify only MAC addresses in the IETF format. In this case, set the MAC address format of Calling-Station-ID to

	IETF.

Configuring the Parsing Mode of the RADIUS Class Attribute

Command	**radius-server attribute class user-flow-control { format-16bytes | format-32bytes }**
Parameter Description	**user-flow-control:** Parses the rate limit configuration from the class attribute. **format-16bytes:** Sets the format of the rate limit value to 16 bytes in the **class** attribute. **format-32bytes:** Sets the format of the rate limit value to 32 bytes in the **class** attribute.
Command Mode	Global configuration mode
Usage Guide	Configure this command if the server needs to issue the rate limit value by using the Class attribute.

Setting the Private Attribute port-priority Issued by the Server to the COS Value of an Interface

Command	**radius set qos cos**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure this command to use the issued QoS value as the CoS value. The QoS value is used as the DSCP value by default.

Configures the Device to Support the CUI Attribute

Command	**radius support cui**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure this command to enable the RADIUS-compliant device to support the CUI attribute.

Configuring the Mode of Parsing Private Attributes by the Device

Command	**Radius vendor-specific extend**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to identify attributes of all vendor IDs by type.

Configuring Whether RADIUS Authentication Request Packets Carry a Specified Attribute

Command	**radius-server authentication attribute** *type* **package** **radius-server authentication attribute** *type* **unpackage**
Parameter Description	***type***: Indicates the RADIUS attribute type. The value ranges from 1 to 255.
Command	Global configuration mode

Mode	
Usage Guide	Use this command to specify the attribute to be carried in authentication request packets.

Configuring Whether RADIUS Accounting Request Packets Carry a Specified Attribute

Command	**radius-server account attribute** *type* **package** **radius-server account attribute** *type* **unpackage**
Parameter Description	***type***: Indicates the RADIUS attribute type. The value ranges from 1 to 255.
Command Mode	Global configuration mode
Usage Guide	Use this command to specify the attribute to be carried in accounting request packets.

Configuring Whether RADIUS Authentication Request Packets Carry the Private Attribute of a Specified Vendor

Command	**radius-server authentication vendor** *vendor_name* **package**
Parameter Description	*vendor_name*: Indicates the vendor name. It can be set to **cmcc**, **Microsoft**, or **cisco**.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure whether authentication request packets carry the private attribute of a specified vendor.

Configuring Whether RADIUS Accounting Request Packets Carry the Private Attribute of a Specified Vendor

Command	**radius-server account vendor** *vendor_name* **package**
Parameter Description	*vendor_name*: Indicates the vendor name. It can be set to **cmcc**, **Microsoft**, or **cisco**.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure whether accounting request packets carry the private attribute of a specified vendor.

Configuring Whether RADIUS Server Parses the Private Attribute of Cisco, Huawei or Microsoft

Command	**radius vendor-specific attribute support** ***vendor_name***
Parameter Description	*vendor_name*: Indicates the vendor name. It can be set to cisco, huawei or ms.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure whether RADIUS server parses the private attribute of Cisco, Huawei or Microsoft.

Configuration Example

Configuring the RADIUS Attribute Type

Scenario	One authentication device
Configuration Steps	● Configure the MAC address format of RADIUS Calling-Station-Id. ● Configure the RADIUS private attribute type. ● Set the QoS value issued by the RADIUS server as the COS value of the interface. ● Configure the RADIUS function to support the CUI attribute. ● Configure the device to support private attributes of other vendors. ● Configure authentication requests not to carry the NAS-PORT-ID attribute. ● Configure accounting requests to carry the CMCC private attribute. ● Configure the RAIUDS server not to parse Cisoc's private attributes contained in packets. ● Configure application of the nas-port-id encapsulation format in a QINQ scenario.
	FS(config)#radius-server attribute 31 mac format ietf FS(config)#radius attribute 16 vendor-type 211 FS(config)#radiussetqoscos FS(config)#radiussupport cui FS(config)#radiusvendor-specific extend FS(config)#radius-server authentication attribute 87 unpackage FS(config)#radius-server account vendor cmcc package FS(config)# no radius vendor-specific attribute support cisco FS(config)# radius-server attribute nas-port-id format qinq
Verification	Conduct packet capture or display debug information of the device to check whether the RADIUS standard attributes and private attributes are encapsulated/parsed correctly.

13.4.3 Configuring RADIUS Accessibility Detection

Configuration Effect

The device maintains the accessibility status of each configured RADIUS server: reachable or unreachable. The device will not transmit authentication, authorization, and accounting requests of access users to an unreachable RADIUS server unless all the other servers in the same RADIUS server group as the unreachable server are all unreachable.

The device actively detects a specified RADIUS server. The active detection function is disabled by default. If the active detection function is enabled for a specified RADIUS server, the device will, according to the configuration, periodically transmits detection requests (authentication requests or accounting requests) to the RADIUS server. The transmission interval is as follows:

- For a reachable RADIUS server, the interval is the active detection interval of the reachable RADIUS server (the default value is 60 minutes).
- For an unreachable RADIUS server, the interval is always 1 minute.

Notes

All the following conditions need to be met before the active detection function is enabled for a specified RADIUS server:

- The test user name of the RADIUS server is configured on the device.
- At least one tested port (authentication port or accounting port) of the RADIUS server is configured on the device.

If the following two conditions are all met, it is deemed that a reachable RADIUS server becomes unreachable:

- After the previous correct response is received from the RADIUS server, the time set in **radius-server dead-criteria time** *seconds* has elapsed.
- After the previous correct response is received from the RADIUS server, the count that the device transmits requests to the RADIUS server but fails to receive correct responses (including retransmission) reaches the value set in **radius-server dead-criteria tries** *number*.

If any of the following conditions is met, it is deemed that an unreachable RADIUS server becomes reachable:

- The device receives correct responses from the RADIUS server.
- The duration that the RADIUS server is in the unreachable state exceeds the time set in **radius-server deadtime** and the active detection function is disabled for the RADIUS server.
- The authentication port or accounting port of the RADIUS server is updated on the device.

Configuration Steps

↘ Configuring the Global Criteria for Judging That a RADIUS Security Server Is Unreachable

- Mandatory.
- Configuring the global criteria for judging that a RADIUS security server is unreachable is a prerequisite for enabling the active detection function.

↘ Configuring the IP Address of the Remote RADIUS Security Server, Authentication Port, Accounting Port, and Active Detection Parameters

- Mandatory.
- Configuring active detection parameters of the RADIUS server is a prerequisite for enabling the active detection function.

↘ Configuring the Duration for the Device to Stop Transmitting Request Packets to an Unreachable RADIUS Server

- Optional.
- The configured duration for the device to stop transmitting request packets to an unreachable RADIUS server takes effect only when the active detection function is disabled for the RADIUS server.

Verification

- Run the **show radius server** command to display the accessibility information of each RADIUS server.

Related Commands

Configuring the Global Criteria for Judging That a RADIUS Security Server Is Unreachable

Command	**radius-server dead-criteria** { **time***seconds* [**tries***number*] | **tries***number* }
Parameter Description	**time***seconds*: Indicates the time condition parameter. If the device fails to receive a correct response packet from a RADIUS security server within the specified time, it is deemed that the RADIUS security server meets the inaccessibility duration condition. The value ranges from 1 second to 120 seconds. **tries***number*: Indicates the consecutive request timeout count. If the timeout count of request packets transmitted by the device to the same RADIUS security server reaches the preset count, it is deemed that the RADIUS security server meets the consecutive timeout count condition of inaccessibility. The value ranges from 1 to 100.
Command Mode	Global configuration mode
Usage Guide	If a RADIUS security server meets both the duration condition and the consecutive request timeout count condition, it is deemed that the RADIUS security server is unreachable. Users can use this command to adjust parameter values in the duration condition and consecutive request timeout count condition.

Configuring the Duration for the Device to Stop Transmitting Request Packets to an Unreachable RADIUS Server

Command	**Radius-server deadtime** *minutes*
Parameter Description	*minutes*: Indicates the duration for the device to stop transmitting requests to an unreachable RADIUS security server, with the unit of minutes. The value ranges from 1 minute to 1,440 minutes (24 hours).
Command Mode	Global configuration mode
Usage Guide	If the active detection function is enabled for a RADIUS security server on the device, the time parameter in **radius-server deadtime** does not take effect on the RADIUS server. If the active detection function is disabled for a RADIUS security server, the device automatically restores the RADIUS security server to the reachable state when the duration that the RADIUS security server is in the unreachable state exceeds the time specified in **radius-server deadtime**.

Configuration Example

Configuring Accessibility Detection on the RADIUS Server

Scenario Figure 13-5	
Configuratio	- Configure the global criteria for judging that a RADIUS security server is unreachable.

n Steps	● Configure the IP address of the remote RADIUS security server, authentication port, accounting port, and active detection parameters.
RADIUS Client	FS(config)#radius-server dead-criteria time120 tries 5 FS(config)# radius-server host 192.168.5.22 test username test ignore-acct-port idle-time 90
Verification	Disconnect the network communication between the device and the server with the IP address of 192.168.5.22.Conduct RADIUS authentication through the device. After 120 seconds, run the **show radius server** command to check that the server state is **dead**.
	FS#show running-config ... radius-server host 192.168.5.22 test username test ignore-acct-port idle-time 90 radius-server dead-criteria time 120 tries 5 ...

13.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears statistics of the RADIUS dynamic authorization extension function and restarts statistics.	**clear radius dynamic-authorization-extension statistics**

Displaying

Description	Command
Displays global parameters of the RADIUS server.	**show radius parameter**
Displays the configuration of the RADIUS server.	**show radius server**
Displays the configuration of the RADIUS private attribute type.	**show radius vendor-specific**
Displays statistics relevant to the RADIUS dynamic authorization extension function.	**show radius dynamic-authorization-extension statistics**
Displays statistics relevant to RADIUS authentication.	**show radius auth statistics**
Displays statistics relevant to RADIUS accounting.	**show radius acct statistics**

Description	Command
Displays configuration of RADIUS server groups.	**show radius group**
Displays RADIUS standard attributes.	**show radius attribute**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the RADIUS event.	**debugradiusevent**
Debugs RADIUS packet printing.	**debugradiusdetail**
Debugs the RADIUS dynamic authorization extension function.	**debug radiusextension event**
Debugs the RADIUS dynamic authorization extension packet printing.	**debug radius extension detail**

14 Configuring TACACS+

14.1 Overview

TACACS+ is a security protocol enhanced in functions based on the Terminal Access Controller Access Control System (TACACS) protocol. It is used to implement the authentication, authorization, and accounting (AAA) of multiple users.

Protocols and Standards

- RFC 1492 Terminal Access Controller Access Control System

14.2 Applications

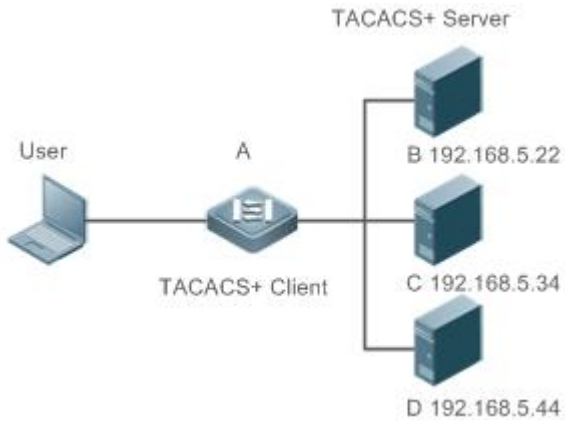
Application	Description
Managing and Controlling Login of End Users	Password verification and authorization need to be conducted on end users.

14.2.1 Managing and Controlling Login of End Users

Scenario

TACACS+ is typically applied in the login management and control of end users. A network device serves as the TACACS+ client and sends a user name and password to the TACACS+ server for verification. The user is allowed to log in to the network device and perform operations after passing the verification and obtaining authorization. See the following figure.

Figure 14-1



Remarks	● A is a client that initiates TACACS+ requests. ● B, C, and D are servers that process TACACS+ requests.

Deployment

- Start the TACACS+ server on Server B, Server C, and Server D, and configure information on the access device (Device A) so that the servers provide TACACS+-based AAA function for the access device. Enable the AAA function on Device A to start authentication for the user login.

- Enable the TACACS+ client function on Device A, add the IP addresses of the TACACS+ servers (Server B, Server C, and Server D) and the shared key so that Device A communicates with the TACACS+ servers over TACACS+ to implement the AAA function.

14.3 Features

Basic Concepts

Format of TACACS+ Packets

Figure 14-2

4	8	16	24	32 bit
Major	Minor	Packet type	Sequence no.	Flags
Session ID				
Length				

- Major Version: Indicates the major TACACS+ version number.
- Minor Version: Indicates the minor TACACS+ version number.
- Packet Type: Indicates the type of packets, with the options including:
- TAC_PLUS_AUTHEN: = 0x01 (authentication);
- TAC_PLUS_AUTHOR: = 0x02 (authorization);
- TAC_PLUS_ACCT: = 0x03 (accounting)
- Sequence Number: Indicates the sequence number of a data packet in the current session. The sequence number of the first TACACS+ data packet in a session must be 1 and the sequence number of subsequent each data packet increases by one. Therefore, the client sends data packets only with an odd sequence number and TACACS+ Daemon sends packets only with an even sequence number.
- Flags: Contains various bitmap format flags. One of the bits in the value specifies whether data packets need to be encrypted.
- Session ID: Indicates the ID of a TACACS+ session.
- Length: Indicates the body length of a TACACS+ data packet (excluding the header). Packets are encrypted for transmission on a network.

Overview

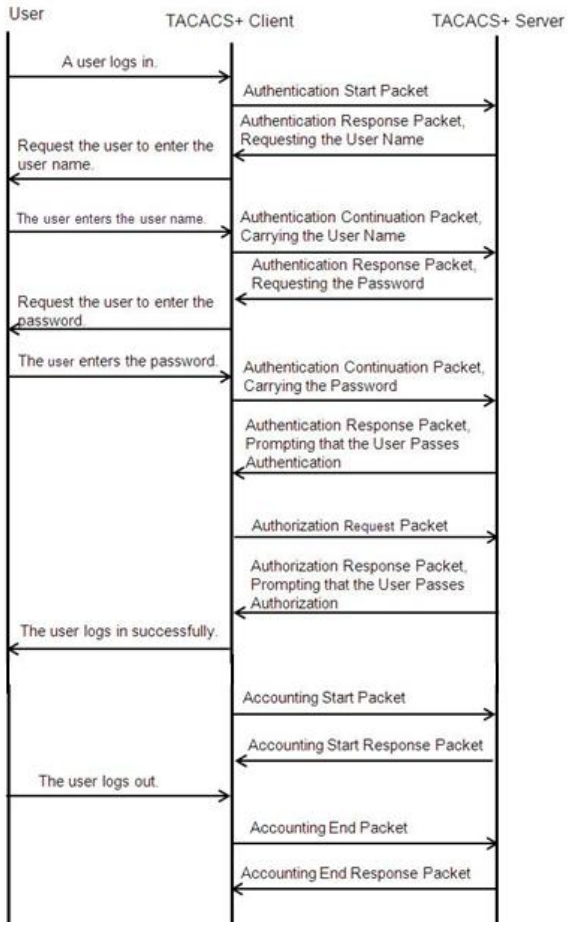
Feature	Description
TACACS+ Authentication, Authorization, and Accounting	Conducts authentication, authorization, and accounting on end users.

14.3.1 TACACS+ Authentication, Authorization, and Accounting

Working Principle

The following figure uses basic authentication, authorization, and accounting of user login to describe interaction of TACACS+ data packets.

Figure 14-3



The entire basic message interaction process includes three sections:

1. The authentication process is described as follows:

   1) A user requests to log in to a network device.

   2) After receiving the request, the TACACS+ client sends an authentication start packet to the TACACS+ server.

   3) The TACACS+ server returns an authentication response packet, requesting the user name.

   4) The TACACS+ client requests the user to enter the user name.

   5) The user enters the login user name.

   6) After receiving the user name, the TACACS+ client sends an authentication continuation packet that carries the user name to the TACACS+ server.

   7) The TACACS+ server returns an authentication response packet, requesting the login password.

   8) The TACACS+ client requests the user to enter the login password.

   9) The user enters the login password.

10) After receiving the login password, the TACACS+ client sends an authentication continuation packet that carries the login password to the TACACS+ server.

11) The TACACS+ server returns an authentication response packet, prompting that the user passes authentication.

Configuration	Description and Command	
Configuring TACACS+ Basic Functions	(Mandatory) It is used to enable the TACACS+ security service.	
	tacacs-server host	Configures the TACACS+ server.
	tacacs-server key	Specifies the key shared by the server and network device.
	tacacs-server timeout	Configures the global waiting timeout time of the TACACS+ server for communication between a network device and the TACACS+ server.
Configuring Separate Processing of Authentication, Authorization, and Accounting of TACACS+	(Optional) It is used to separately process authentication, authorization, and accounting requests.	
	aaa group server tacacs+	Configures TACACS+ server groups and divides TACACS+ servers into different groups.
	server	Adds servers to TACACS+ server groups.

2. The user authorization starts after successful authentication:

   1) The TACACS+ client sends an authorization request packet to the TACACS+ server.

   2) The TACACS+ server returns an authorization response packet, prompting that the user passes authorization.

   3) After receiving the authorization success packet, the TACACS+ client outputs the network device configuration screen for the user.

3. Accounting and audit need to be conducted on the login user after successful authorization:

   1) The TACACS+ client sends an accounting start packet to the TACACS+ server.

   2) The TACACS+ server returns an accounting response packet, prompting that the accounting start packet has been received.

   3) The user logs out.

   4) The TACACS+ client sends an accounting end packet to the TACACS+ server.

   5) The TACACS+ server returns an accounting response packet, prompting that the accounting end packet has been received.

14.4 Configuration

14.4.1 Configuring TACACS+ Basic Functions

Configuration Effect

- The TACACS+ basic functions are available after the configuration is complete. When configuring the AAA method list, specify the method of using TACACS+ to implement TACACS+ authentication, authorization, and accounting.
- When authentication, authorization, and accounting operations are performed, TACACS+ initiates the authentication, authorization, and accounting requests to configured TACACS+ servers according to the configured sequence. If response timeout occurs on a TACACS+ server, TACACS+ traverses the TACACS+ server list in sequence.

Notes

- The TACACS+ security service is a type of AAA service. You need to run the **aaa new-model** command to enable the security service.
- Only one security service is provided after TACACS+ basic functions are configured. To make the TACACS+ functions take effect, specify the TACACS+ service when configuring the AAA method list.

Configuration Steps

Enabling AAA

- Mandatory. The AAA method list can be configured only after AAA is enabled. TACACS+ provides services according to the AAA method list.

Command	**aaa new-model**
Parameter Description	N/A
Defaults	The AAA function is disabled.
Command Mode	Global configuration mode
Usage Guide	The AAA method list can be configured only after AAA is enabled. TACACS+ provides services according to the AAA method list.

Configuring the IP Address of the TACACS+ Server

- Mandatory. Otherwise, a device cannot communicate with the TACACS+ server to implement the AAA function.

Command	**tacacs-server host** [**oob**] {*ipv4-address* } [**port***integer*] [**timeout** *integer*][**key** [**0** | **7**] *text-string*]
Parameter Description	*ipv4-address*: Indicates the IPv4 address of the TACACS+ server. **oob**: Uses an MGMT port as the source interface for communicating with the TACACS+ server. A non-MGMT port is used for communication by default. **port***integer*: Indicates the TCP port used for TACACS+ communication. The default TCP port is 49. **timeout** *integer*: Indicates the timeout time of the communication with the TACACS+ server. The global timeout time is used by default. **key** [**0** | **7**] *text-string*: Indicates the shared key of the server. The global key is used if it is not configured. An encryption type can be specified for the configured key. The value **0** indicates no encryption and **7** indicates simple encryption. The default value is **0**.
Defaults	No TACACS+ server is configured.
Command	Global configuration mode

Mode	
Usage Guide	4. You can specify the shared key of the server when configuring the IP address of the server. If no shared key is specified, the global key configured using the **tacacs-server key** command is used as the shared key of the server. The shared key must be completely the same as that configured on the server. 5. You can specify the communication port of the server when configuring the IP address. 6. You can specify the communication timeout time of the server when configuring the IP address.

Configuring the Shared Key of the TACACS+ Server

- Optional.
- If no global communication protocol is configured using this command, set **key** to specify the shared key of the server when running the **tacacs-server host** command to add server information. Otherwise, a device cannot communicate with the TACACS+ server.
- If no shared key is specified by using **key** when you run the **tacacs-server host** command to add server information, the global key is used.

Command	**tacacs-server** [**key** [**0** | **7**] *text-string*]
Parameter Description	*text-string*: Indicates the text of the shared key. **0 | 7**: Indicates the encryption type of the key. The value **0** indicates no encryption and **7** indicates simple encryption.
Defaults	No shared key is configured for any TACACS+ server.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure a global shared key for servers. To specify a different key for each server, set **key** when running the **tacacs-server host** command.

Configuring the Timeout Time of the TACACS+ Server

- Optional.
- You can set the timeout time to a large value when the link between the device and the server is unstable.

Command	**tacacs-server timeout** *seconds*
Parameter Description	*seconds*: Indicates the timeout time, with the unit of seconds. The value ranges from 1 second to 1,000 seconds.
Defaults	The default value is 5 seconds.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the global server response timeout time. To set different timeout time for each server, set **timeout** when running the **tacacs-server host** command.

Verification

Configure the AAA method list that specifies to conduct authentication, authorization, and accounting on users by using TACACS+.

- Enable the device to interact with the TACACS+ server and conduct packet capture to check the TACACS+ interaction process between the device and the TACACS+ server.
- View server logs to check whether the authentication, authorization, and accounting are normal.

Configuration Example

Using TACACS+ for Login Authentication

Scenario Figure 14-4	
Remarks	● A is a client that initiates TACACS+ requests. ● B is a server that processes TACACS+ requests.
Configuration Steps	● Enable AAA. ● Configure the TACACS+ server information. ● Configure the method of using TACACS+ for authentication. ● Apply the configured authentication method on an interface.
A	FS# configure terminal FS(config)# aaa new-model FS(config)# tacacs-server host 192.168.5.22 FS(config)# tacacs-server key aaa FS(config)# aaa authentication login test group tacacs+ FS(config)# line vty 0 4 FS(config-line)# login authentication test
Verification	Telnet to a device from a PC. The screen requesting the user name and password is displayed. Enter the correct user name and password to log in to the device. View the authentication log of the user on the TACACS+ server.

Common Errors

- The AAA security service is disabled.
- The key configured on the device is inconsistent with the key configured on the server.
- No method list is configured.

14.4.2 Configuring Separate Processing of Authentication, Authorization, and Accounting of TACACS+

Configuration Effect

- The authentication, authorization, and accounting in the security service are processed by different TACACS+ servers, which improves security and achieves load balancing to a certain extent.

Notes

- The TACACS+ security service is a type of AAA service. You need to run the **aaa new-model** command to enable the security service.
- Only one security service is provided after TACACS+ basic functions are configured. To make the TACACS+ functions take effect, specify the TACACS+ service when configuring the AAA method list.

Configuration Steps

Configuring TACACS+ Server Groups

- Mandatory. There is only one TACACS+ server group by default, which cannot implement separate processing of authentication, authorization, and accounting.
- Three TACACS+ server groups need to be configured for separately processing authentication, authorization, and accounting.

Command	**aaa group server tacacs+***group-name*
Parameter Description	*group-name*: Indicates the name of a group. A group name cannot be radius or tacacs+, which are the names of embedded groups.
Defaults	No TACACS+ server group is configured.
Command Mode	Global configuration mode
Usage Guide	Group TACACS+ servers so that authentication, authorization, and accounting are completed by different server groups.

Adding Servers to TACACS+ Server Groups

- Mandatory. If no server is added to a server group, a device cannot communicate with TACACS+ servers.
- In server group configuration mode, add the servers that are configured using the **tacacs-server host** command.

Command	**server {***ipv4-address* **}**
Parameter Description	*ipv4-address*: Indicates the IPv4 address of the TACACS+ server.
Defaults	No server is configured.
Command Mode	TACACS+ server group configuration mode
Usage Guide	Before configuring this command, you must run the **aaa group server tacacs+** command to enter the TACACS+ server group configuration mode. For the address of a server configured in a TACACS+ server group, the server must be configured using the **tacacs-server host** command in global configuration mode.

	If multiple servers are added to one server group, when one server does not respond, the device continues to send a TACACS+ request to another server in the server group.

Configuring oob of a TACACS+ Server Group

- Optional. Configure oob if a device needs to send TACACS+ packets through a specified MGMT port.
- In server group configuration mode, specify routing for the communication of servers in the group.

Command	**ip oob via**
Parameter Description	**oob** : Using MGMT 0
Defaults	No oob is specified by default.
Command Mode	TACACS+ server group configuration mode
Usage Guide	Before configuring this command, you must run the **aaa group server tacacs+** command to enter the TACACS+ server group configuration mode. If no MGMT port is specified, the MGMT0 port is used by default.

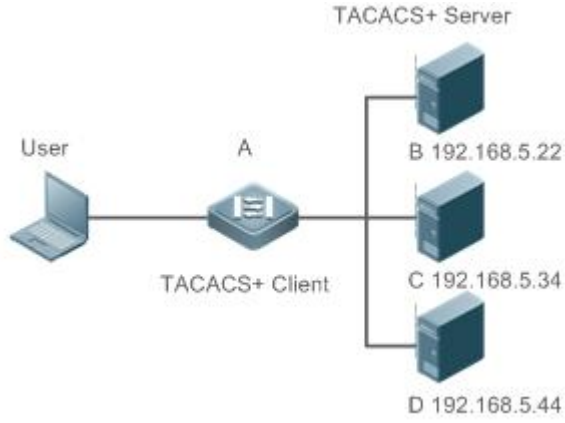
Verification

Configure the AAA method list that specifies to conduct authentication, authorization, and accounting on users by using TACACS+.

- Enable a device to interact with TACACS+ servers. Conduct packet capture, check that the authentication, authorization, and accounting packets are interacted with different servers, and check the source addresses in packets.

Configuration Example

Configuring Different TACACS+ Server Groups for Separately Processing Authentication, Authorization, and Accounting

Scenario **Figure 14-5**	
Remarks	● A is a client that initiates TACACS+ requests. ● B is a server that processes TACACS+ authentication requests. ● C is a server that processes TACACS+ authorization requests.

	● D is a server that processes TACACS+ accounting requests.
Configuration Steps	● Enable AAA. ● Configure the TACACS+ server information. ● Configure TACACS+ server groups. ● Add servers to TACACS+ server groups. ● Configure the method of using TACACS+ for authentication. ● Configure the method of using TACACS+ for authorization. ● Configure the method of using TACACS+ for accounting. ● Apply the configured authentication method on an interface. ● Apply the configured authorization method on an interface. ● Apply the configured accounting method on an interface.
	FS# configure terminal FS(FS(config)# aaa new-model FS(config)# tacacs-server host 192.168.5.22 FS(config)# tacacs-server host 192.168.5.34 FS(config)# tacacs-server host 192.168.5.44 FS(config)# tacacs-server key aaa FS(config)# aaa group server tacacs+ tacgrp1 FS(config-gs-tacacs)# server 192.168.5.22 FS(config-gs-tacacs)# exit FS(config)# aaa group server tacacs+ tacgrp2 FS(config-gs-tacacs)# server 192.168.5.34 FS(config-gs-tacacs)# exit FS(config)# aaa group server tacacs+ tacgrp3 FS(config-gs-tacacs)# server 192.168.5.44 FS(config-gs-tacacs)# exit FS(config)# aaa authentication login test1 group tacacs+ FS(config)# aaa authentication enable default group tacgrp1 FS(config)# aaa authorization exec test2 group tacgrp2 FS(config)# aaa accounting commands 15 test3 start-stop group tacgrp3 FS(config)# line vty 0 4 FS(config-line)# login authentication test1 FS(config-line)#authorization exec test2 FS(config-line)# accounting commands 15 test3
Verification	Telnet to a device from a PC. The screen requesting the user name and password is displayed.

	Enter the correct user name and password to log in to the device. Enter the **enable** command and enter the correct **enable** password to initiate **enable** authentication. Enter the privilege EXEC mode after passing the authentication. Perform operations on the device and then exit the device. View the authentication log of the user on the server with the IP address of 192.168.5.22. View the **enable** authentication log of the user on the server with the IP address of 192.168.5.22. View the **exec** authorization log of the user on the server with the IP address of 192.168.5.34. View the command accounting log of the user on the server with the IP address of 192.168.5.44.

Common Errors

- The AAA security service is disabled.
- The key configured on the device is inconsistent with the key configured on the server.
- Undefined servers are added to a server group.
- No method list is configured.

14.5 Monitoring

Displaying

Description	Command
Displays interaction with each TACACS+ server.	**show tacacs**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs TACACS+.	**debug tacacs+**

15 Configuring Web Authentication

15.1 Overview

15.1.1 Web Authentication

Web authentication controls user access to networks. It requires no authentication software on clients. Instead, users can perform authentication on common browsers.

When unauthenticated clients attempt to access the Internet using browsers, the network access server (NAS) forcibly redirects the browsers to a specified site pointing to a Web authentication server, also called a portal server. Users can access the services on the portal server before being authenticated, such as downloading security patches and reading notices. If a user wants to access network resources beyond the portal server, the user must get authenticated by the portal server through a browser.

Besides providing convenient authentication, the portal server performs Webpage interaction with browsers, providing personalized services, such as advertisements, notices, and business links on the authentication page.

FS Web Authentication Versions

There are three versions of FS Web authentication, including FS First-Generation Web Authentication, FS Second-Generation Web Authentication, and FS Internal Portal (iPortal) Web Authentication. The Web authentication process varies with authentication versions. For details, see Section 15.3 "Features".

- The three versions of Web authentication are highly divergent in features and configurations. It is recommended to read through the relevant chapters carefully before configuration.
- Both FS Second-Generation Web Authentication and FS iPortal Web Authentication support local account authentication on the NAS. Because Remote Authentication Dial In User Service (RADIUS) authentication is more commonly used in reality, it is used as an example in the chapter "Applications".
- The concept of "interface" varies with product types. For example, the interfaces on a layer-2 switch are physical ports; the interfaces on a router may be sub interfaces; the interfaces on wireless devices may represent a wireless local area network (WLAN). This document uses the unified term "interface" to include them. In application, recognize the real meaning based on specific products and functions.
- Web authentication supports user online traffic detection. For details, see the Configuring Layer23.
- This document describes the configuration of Web authentication mainly in interface configuration mode. For FS EG products, Web authentication is configured in global configuration mode. Make sure to enter the correct configuration mode.
- Web authentication supports the authentication of domain names. That is, accounts can be authenticated in the format of user name@domain name. This requires enabling the domain-name-based authentication, authorization and accounting (AAA) service. For details, see the Configuring AAA.

Protocols and Standards

- HTTP: RFC1945 and RFC2068

- HTTPS: RFC2818
- SNMP: RFC1157 and RFC 2578
- RADIUS: RFC2865, RFC2866, and RFC3576
- For the standards related to MAC SMS authentication, see the *CMCC WLAN Device Interface Standards V3.1.0_20130901 (MAC Address-Based Authentication Extension), Zhejiang CMCCWLAN Fast Authentication Scheme – Interface Standards V1.1-2011.3.22*, and *WLAN Fast MAC Address-Based SMS Authentication Scheme V1.1-2011.3.21*.

15.2 Applications

Application	Description
Basic Scenario of Web Authentication	Basic layer-2 authentication scenario, where a NAS, portal server, and RADIUS server constitute an authentication system which connects a client with the NAS through the layer-2 network.

15.2.1 Basic Scenario of Web Authentication

Scenario

See Figure 15-1.

- Deploy a Web authentication scheme on the NAS.
- The client connected to the NAS needs to pass Web authentication before accessing the Internet.

Figure 15-1 Networking Topology of Web Authentication

Remarks	Web authentication is applicable to both layer-2 and layer-3 networks. At layer 3, the source MAC address and VID of a packet are changed after it is routed, but the source IP address remains the same as the only identifier of a client. Therefore, the binding policy of Web authentication on layer-3 devices must adopt the IP-only binding mode. Here, layer-2 NAS is used as an example. FS-SAM program is installed on the RADIUS server. FS-ePortal program is installed on the portal server.

Deployment

- Enable Web authentication on the client-accessed interface or globally on the NAS (globally on EG devices).

- Configure the ePortal server and the communication key on the NAS (for only FS First-Generation and Second-Generation Web Authentication).
- Configure the Simple Network Management Protocol (SNMP) communication parameters of the ePortal server on the NAS (for only FS First-Generation and Second-Generation Web Authentication).
- Configure the consistent communication parameters on the ePortal server and SAM server (for only FS First-Generation Web Authentication).
- Create user accounts on the SAM server.
- Configure AAA and method lists on the NAS (for only FS Second-Generation and iPortal Web Authentication).
- Configure the IP address of the SAM server on the NAS (for only FS Second-Generation and iPortal Web Authentication).
- Configure the names of the Web authentication method lists on the NAS (for only FS Second-Generation and iPortal Web Authentication).

15.3 Features

Basic Concepts

FS First-Generation Web Authentication

FS First-Generation Web Authentication should cooperate with the FS-ePortal software. The server installed with FS-ePortal provides a login page to submit user authentication information, and initiates an authentication request to the RADIUS server directly. After authentication succeeds, the NAS gets user information delivered through the SNMP protocol, and thereby controls user access permissions. Communication during Web authentication of this version depends on private SNMP nodes. Moreover, the ePortal server takes the place of the NAS in authentication and accounting, which relieves the NAS from service burden.

FS Second-Generation Web Authentication

FS Second-Generation Web Authentication complies with the *CMCC WLAN Service Portal Specification*. The portal server is responsible only for Webpage interaction with users. The NAS interacts with the RADIUS server to implement authentication. The interaction between the portal server and the NAS complies with the *CMCC WLAN Service Portal Specification*. The portal server provides a login page for users to submit their information, and informs the NAS of user information through the portal protocols. The NAS completes authentication by interacting with the RADIUS server based on the user information, assigns access permissions to authenticated clients, and returns authentication results to the portal server.

The implementation process of FS Second-Generation Web Authentication is mainly completed on the NAS. This raises a higher demand on the NAS's capability to handle heavy tasks. Meanwhile, the portal server is simplified. The standard *CMCC WLAN Service Portal Specification*, which gains highly industry support, enables various vendors to develop compatible products.

FS iPortal Web Authentication

In FS iPortal Web Authentication, the NAS integrates Webpage interaction of the portal server and partial authentication interaction of the RADIUS server. The NAS has a default authentication page suite. It can be customized according to the configuration described in this manual. Then, download the configured page suite to the storage medium of the NAS for effect.

Version Comparison

Authentication roles:

- Client: Its functions are the same among the three types of Web authentication.
- NAS: In FS First-Generation Web Authentication, the NAS implements only URL redirection and exchanges user login/logout notifications with the portal server. In FS Second-Generation Web Authentication, the NAS is responsible for redirecting and authenticating users as well as notifying the portal server of authentication results. In FS iPortal Web authentication, the NAS integrates multiple functions including the URL redirection, Webpage interaction, and authentication.
- Portal server: In FS First-Generation Web Authentication, the portal server is responsible for interaction with clients through Webpages, authenticating users, and notifying the NAS of authentication results. In FS Second-Generation Web Authentication, the portal server is responsible for interacting with clients through Webpages, notifying the NAS of users' authentication information, and receiving authentication results from the NAS. In FS iPortal Web Authentication, the portal server is built into the NAS and provides simplified functions, mainly responsible for Web page interaction with clients.
- RADIUS server: Its functions are the same among the three types of Web authentication.

Authentication process:

- FS iPortal Web Authentication simplifies and integrates the features of the first- and second-generation portal servers into the NAS.

Logout process:

- In FS First-Generation Web Authentication, a logout action may be triggered by a notification from the portal server, or traffic detection or port status detection performed by the NAS. In FS Second-Generation Web Authentication, a logout action may be triggered by a notification from the portal server, a kickout notification from the RADIUS server, or traffic detection or port status detection performed by the NAS. In FS iPortal Web Authentication, a logout action may be triggered by the voluntary logout of a user through clicking the **Logout** button on the online page, a kickout notification from the RADIUS server, or traffic detection or port status detection performed by the NAS.
- In FS First-Generation Web Authentication, Accounting Stop packets are sent by the portal server. In FS Second-Generation Web Authentication, Accounting Stop packets are sent by the NAS, the same as FS iPortal Web Authentication.

The selection of the Web authentication versions depends on the type of the portal server in use.

Command parameters in this document may be shared by the three Web authentication versions or not. Read through this document carefully to avoid parameter misconfiguration that will affect Web authentication.

Overview

Feature	Description
FS First-Generation Web Authentication	The portal server is deployed and supports only FS First-Generation Web Authentication.
FS Second-Generation Web Authentication	The portal server is deployed and complies with the *CMCC WLAN Service Portal Specification*.
FS iPortal Web Authentication	The portal server is not deployed, and the NAS supports Webpage interaction.

15.3.1 FS First-Generation Web Authentication

HTTP Interception

HTTP interception means the NAS intercepts to-be-forwarded HTTP packets. Such HTTP packets are initiated by the browsers of the clients connected to the NAS, but they are not destined for the NAS. For example, when a client attempts to visit the website www.google.com using the Internet Explorer, the NAS is expected to forward the HTTP request packets to the gateway. If HTTP interception is enabled, these packets will not be forwarded.

After HTTP interception is successful, the NAS redirects the HTTP requests from the client to itself to establish a session between them. Then, the NAS pushes a Webpage to the client through HTTP redirection, which can be used for authentication, software downloading or other purposes.

You can specify the clients and destination interfaces to enable or disable HTTP interception for Web authentication. In general, HTTP requests from unauthenticated clients will be intercepted, and those from authenticated clients will not. HTTP interception is the foundation of Web authentication. Web authentication is automatically triggered once HTTP interception succeeds.

HTTP Redirection

According to HTTP protocols, after the NAS receives a HTTP GET or HEAD request packet from a client, a packet with 200 (Ok) status code is replied if it is able to provide the required resources, or a packet with 302 (Moved Temporarily) status code is returned if unable. Another URL is provided in the 302 packet. After receiving the packet, the client may resend a HTTP GET or HEAD request packet to the new URL for requesting resources. This process is called redirection.

HTTP redirection is an important procedure following HTTP interception in Web authentication. It takes the advantage of 302 status code defined in HTTP protocols. HTTP interception creates a session between the NAS and a client. The client sends HTTP GET or HEAD request packets (which should have been sent to another site) to the NAS. The NAS responds with a 302 packet with a specific redirection page. Thereby, the client resends the requests to the redirection page.

Because more and more application programs run HTTP protocols, the use of the 302 redirection packet may divert a large amount of HTTP traffic (not sent by browsers) to the portal server, which will affect network authentication. To address this problem, HTTP redirection technology on the NAS adopts noise reduction to replace the 302 packets with the **js** script.

Working Principle

Figure 15- 1 shows the networking topology of Web authentication.

First-generation Webauth roles:

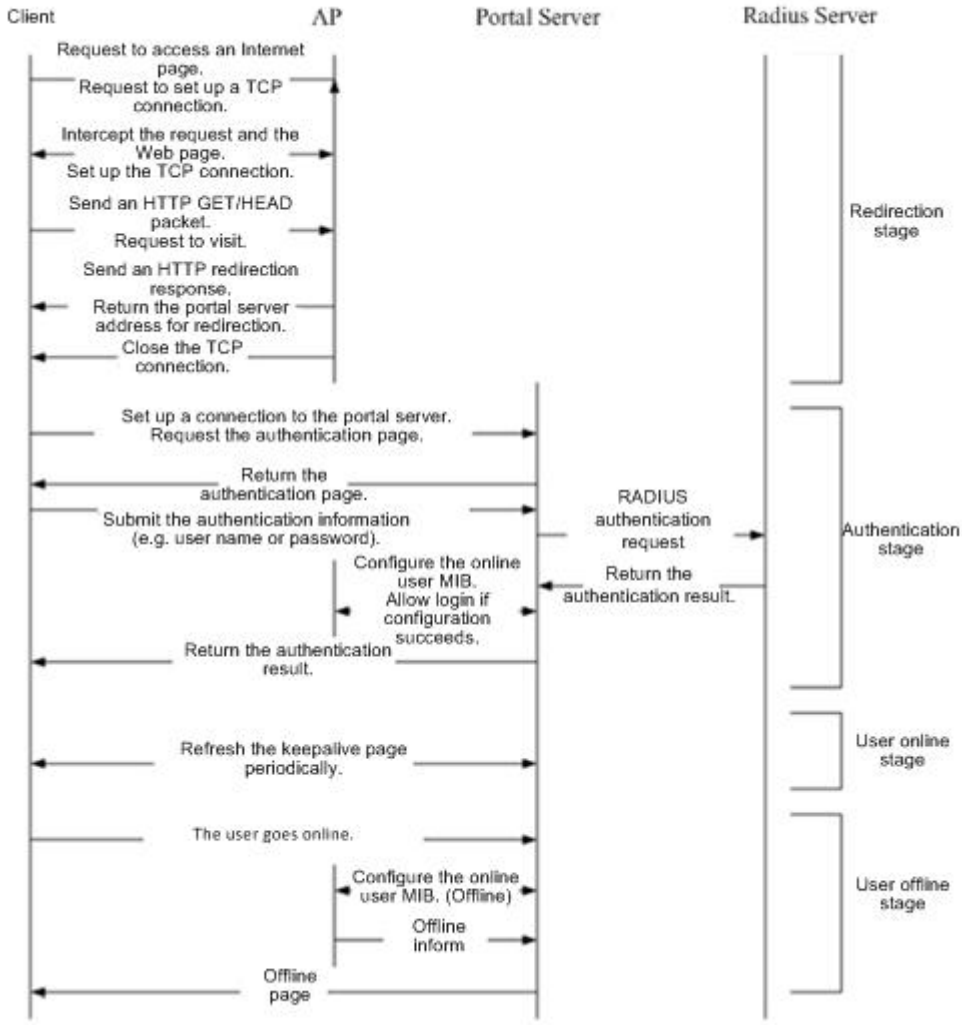
1. Authentication client: Is usually a browser running HTTP protocols. It sends HTTP requests for accessing the Internet.
2. NAS: Is an access-layer device in a network (for example, a wireless access point [AP] on a wireless network). The NAS is directly connected to clients and must be enabled with Web authentication.
3. Portal server: Provides a Web page for Web authentication and related operations. After receiving an HTTP authentication request from a client, the portal server extracts account information from the request, sends the information to the RADIUS server for authentication, and notifies the client and NAS of the authentication result. Figure 15-1 shows FS ePortal server.
4. RADIUS server: Provides the RADIUS-based authentication service to remote clients. The portal server extracts users' authentication account information from HTTP packets and initiates authentication requests to the RADIUS server through the RADIUS protocol. The RADIUS server returns the authentication result to the portal server through the RADIUS protocol. Figure 15-1 shows the RADIUS server installed with the FS-SAM program.

First-generation Webauth process:

1. Before authentication, the NAS intercepts all HTTP requests from a client and redirects these requests to the iPortal server. Thereafter, an authentication page is displayed on the browser.
2. During authentication, the client enters information, for example, username, password, and verification code, on the Webauth URL to interact with the portal server and complete authentication.
3. After the user is authenticated, the portal server notifies the NAS that the client has passed authentication, and the NAS allows the client to access resources on the Internet.

Figure 15-2 shows the flowchart of FS First-Generation Web Authentication by using an AP as the NAS.

Figure 15-2 Flowchart of FS First-Generation Web Authentication



First-generation client logout process:

There are two scenarios of client logout. One scenario is detected by the NAS that a client gets offline for the maximum online time is out, the upper traffic limit is reached, or the link is disconnected. The other scenario is detected by the portal server that a client logs out by clicking the **Logout** button on the logout page or the keep-alive page is invalid.

1. Scenario 1: The NAS detects a client to logout and informs the portal server. Then the portal server deletes the user information on the NAS through SNMP and displays a logout page to the client.
2. Scenario 2: The portal server detects a client to logout and informs the NAS through SNMP and displays a logout page to the client.
3. In the two scenarios, the portal server sends an Accounting Stop request to the RADIUS server and notifies the RADIUS server that the client has logged out.

Related Configuration

↘ Configuring the First-Generation Webauth Template

By default, the first-generation Webauth template is not configured.

Run the **web-auth template eportalv1** command in global configuration mode to create the first-generation Webauth template.

The template is used to implement Web authentication.

Configuring the IP Address of the Portal Server

By default, the IP address of the portal server is not configured.

Run the **ip** {*ip-address* } command in template configuration mode to configure the IP address of the portal server.

Any request packets to access the portal server will be filtered and rate-limited by the NAS.

Configuring the Webauth URL of the Portal Server

By default, the Webauth URL of the portal server is not configured.

Run the **url** {*url-string* } command in template configuration mode to configure the Webauth URL of the portal server.

The URL to which clients are redirected is the address of the Webauth URL provided by the portal server.

Specifying the Webauth Binding Mode

The default Webauth binding mode is IP-MAC binding mode.

Run the **bindmode** command in template configuration mode to specify the Webauth binding mode.

In Web authentication on layer-3 networks, the source MAC address in a packet is changed after the packet is routed. In such case, configure the IP-only binding mode.

Configuring the Webauth Communication Key

By default, the Webauth communication key is not configured.

Run the **web-auth portal key** {*string* } command in global configuration mode to configure the Webauth communication key.

The communication key is used to encrypt URL parameters to avoid information disclosure.

Enabling FS First-Generation Web Authentication

By default, FS First-Generation Web Authentication is disabled.

Run the **web-auth enable** command in global configuration mode to enable FS First-Generation Web Authentication on the client-connected ports.

After Web authentication is enabled, the unauthenticated clients connecting to a port will be redirected to the Webauth URL.

Configuring the SNMP-Server Host

By default, the SNMP-server host and community string are not configured.

Run the **snmp-server host** {*ip-address* }**version 2c** {*community-string* }**web-auth** command in global configuration mode to configure the SNMP-server host and community string for Web authentication.

The SNMP-server host is configured to receive Inform/Trap packets of user logout.

Configuring the SNMP-Server Community String

By default, the SNMP-server community string is not configured.

Run the **snmp-server community** {*community-string*} **rw** command in global configuration mode to configure the SNMP-server community string.

The SNMP-server community string is configured to read/write user information from/to the NAS.

Enabling the SNMP Trap/Inform Function

By default, the SNMP Trap/Inform function is disabled.

Run the **snmp-server enable traps web-auth** command in global configuration mode to enable the SNMP Trap/Inform function.

The SNMP Trap/Inform function is configured to enable the NAS to inform the portal server of user logout.

15.3.2 FS Second-Generation Web Authentication

HTTP Interception

Same as the HTTP interception technology of FS First-Generation Web Authentication.

HTTP Redirection

Same as the HTTP redirection technology of FS First-Generation Web Authentication.

Working Principle

Figure 15- 1 shows the networking topology of Web authentication.

Second-generation Webauth roles:

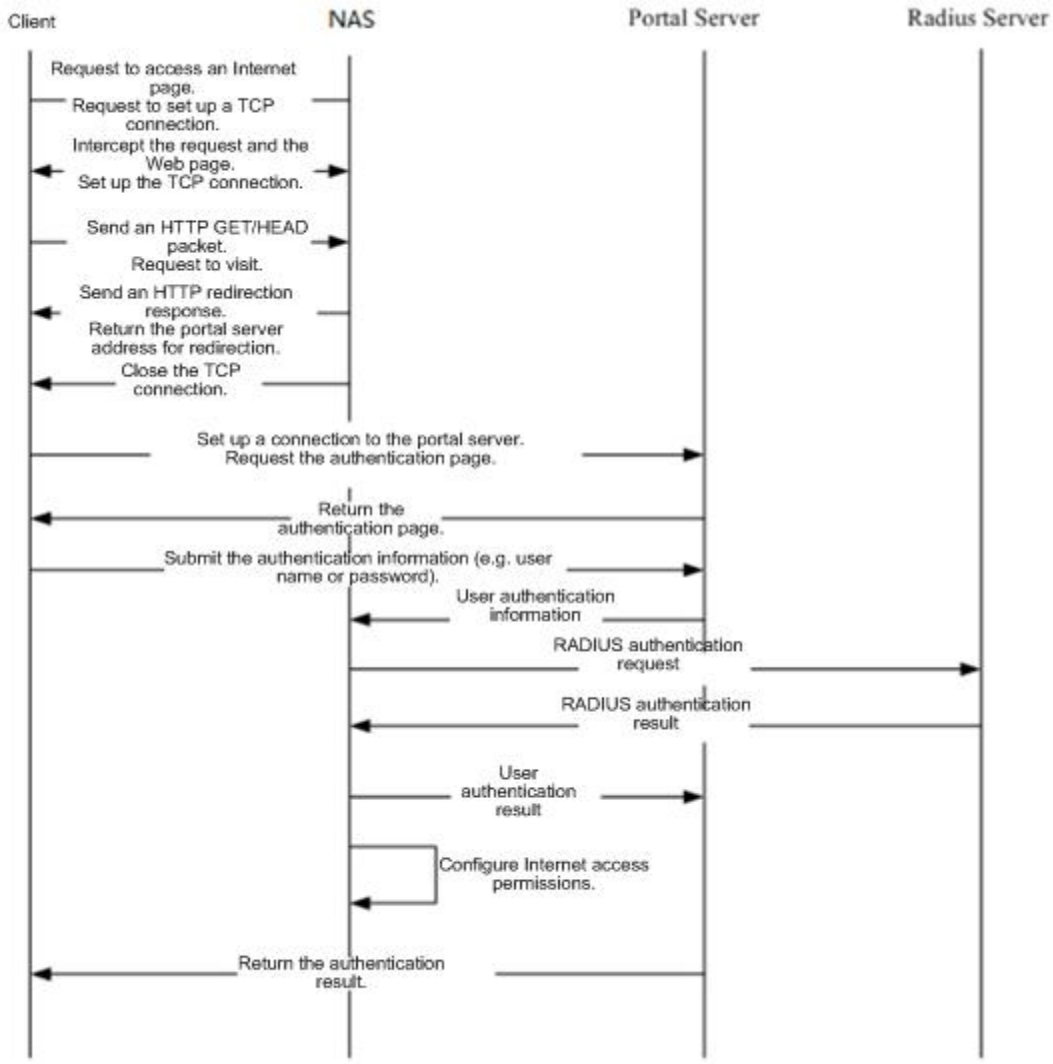
1. Authentication client: Is usually a browser running HTTP protocols. It sends HTTP requests for accessing the Internet.
2. NAS: Is an access-layer device in a network (for example, an AP on a wireless network). The NAS is directly connected to clients and must be enabled with Web authentication. The NAS receives user authentication information from the portal server, sends authentication requests to the RADIUS server, determines whether users can access the Internet according to authentication results, and returns the authentication results to the portal server.
3. Portal server: Provides a Web page for Web authentication and related operations. After receiving an HTTP authentication request from a client, the portal server extracts account information from the request, transfers the information to the NAS, and displays the authentication result returned by the NAS to the user on a page. Figure 15- 1 shows FS ePortal server.
4. RADIUS server: Provides the RADIUS-based authentication service to remote clients. Figure 15- 1 shows the RADIUS server installed with the FS-SAM program.

Second-generation Webauth process:

1. Before authentication, the NAS intercepts all HTTP requests from a client and redirects these requests to the iPortal server. Thereafter, an authentication page is displayed on the browser.
2. During authentication, the client enters information, for example, username, password, and verification code, on the Webauth URL to interact with the portal server.

3. The portal server sends the user authentication information to the NAS.
4. The NAS initiates authentication to the RADIUS server and returns the authentication result to the portal server.
5. The portal server displays the authentication result (success or failure) to the user on a page.

Figure 15-3 Flowchart of FS Second-Generation Web Authentication



Second-generation client logout process:

There are two scenarios of client logout. One scenario is detected by the NAS that a client gets offline for the maximum online time is out, the upper traffic limit is reached, or the link is disconnected. The other scenario is detected by the portal server that a client logs out by clicking the **Logout** button on the logout page or the keep-alive page is invalid.

1. When a user clicks the **Logout** button on the online page, the portal server notifies the NAS to get the user offline.
2. The NAS gets a client offline with traffic lower than the threshold based on the parameters of user online traffic detection.

3. When the RADIUS server plans to force a client offline based on a certain policy, the NAS notifies the portal server to push a logout page to the client.

Related Configuration

Configuring the Second-Generation Webauth Template

By default, the second-generation Webauth template is not configured.

Run the **web-auth template{eportalv2 |** *template-name* **v2}** command in global configuration mode to create a second-generation Webauth template.

The template is used to implement Web authentication.

Configuring the IP Address of the Portal Server

By default, the IP address of the portal server is not configured.

Run the **ip** { *ip-address* } command in template configuration mode to configure the IP address of the portal server.

Any request packets to access the portal server will be filtered and rate-limited by the NAS.

Configuring the Webauth URL of the Portal Server

By default, the Webauth URL of the portal server is not configured.

Run the **url** {*url-string* } command in template configuration mode to configure the Webauth URL of the portal server.

The URL to which clients are redirected is the address of the Webauth URL provided by the portal server.

Specifying the Webauth Binding Mode

The default Webauth binding mode is IP-MAC binding mode.

Run the **bindmode** command in template configuration mode to specify the Webauth binding mode.

In Web authentication on layer-3 networks, the source MAC address in a packet is changed after the packet is routed. In such case, configure the IP-only binding mode.

Configuring the Webauth Communication Key

By default, the Webauth communication key is not configured.

Run the **web-auth portal key** { *string* } command in global configuration mode to configure the Webauth communication key.

The communication key is used to encrypt URL parameters to avoid information disclosure.

Enabling FS Second-Generation Web Authentication

By default, FS Second-Generation Web Authentication is disabled.

Run the **web-auth enable** command in global configuration mode to enable FS Second-Generation Web Authentication on the client-connected ports.

After Web authentication is enabled, the unauthenticated clients connecting to a port will be redirected to the Webauth URL.

Enabling AAA

By default, AAA is disabled.

Run the **aaa new-model** command in global configuration mode to enable AAA.

FS Second-Generation Web Authentication relies on AAA. Enable AAA before you implement the former.

Configuring the RADIUS-Server Host and Communication Key

By default, the RADIUS-server host and communication key are not configured.

Run the **radius-server host** command in global configuration mode to configure the RADIUS-server host and communication key.

The RADIUS-server host is responsible for authenticating users.

Configuring an AAA Method List for FS Second-Generation Web Authentication

By default, no AAA method list is configured for FS Second-Generation Web Authentication.

Run the **aaa authentication web-auth** command in global configuration mode to configure an AAA method list for FS Second-Generation Web Authentication.

The AAA authentication method list is used for interaction during the Webauth process.

Configuring an AAA Method List for FS Second-Generation Web Accounting

By default, no AAA method list is configured for FS Second-Generation Web Accounting.

Run the **aaa accounting network** command in global configuration mode to configure an AAA method list for FS Second-Generation Web Accounting.

The AAA method list for Web accounting is used for accounting interaction during the Webauth process.

Specifying an AAA Method List

The default AAA method list is used if no list is specified.

Run the **authentication** command in template configuration mode to specify an AAA method list.

The AAA method list is specified to send authentication requests to AAA.

Specifying an AAA Accounting Method List

The default AAA accounting method list is used if no list is specified.

Run the **accounting** command in template configuration mode to specify an AAA accounting method list.

The AAA accounting method list is specified to send accounting requests to AAA.

Specifying the UDP Port of the Portal Server

By default, UDP Port 50100 is used.

Run the **port** command in template configuration mode to specify the UDP port of the portal server.

The UDP port is specified for the portal server to communicate with the NAS.

15.3.3 FS iPortal Web Authentication

HTTP Interception

Same as the HTTP interception technology of FS First-Generation Web Authentication.

HTTP Redirection

Same as the HTTP redirection technology of FS First-Generation Web Authentication.

Working Principle

Compared with FS First-Generation Web Authentication shown in Figure 15- 1, FS iPortal Web Authentication does not require the portal server.

iPortal Webauth roles:

1. Authentication client: Is usually a browser running HTTP protocols. It sends HTTP requests for accessing the Internet.
2. NAS: Is an access-layer device in a network. It is directly connected to clients in wired or wireless networks and must be enabled with FS iPortal Web Authentication. The NAS resolves the account information that clients enter on a Webpage and sends authentication requests to the RADIUS server. It determines whether clients can access the Internet according to authentication results and pushes the authentication results to the browsers.
3. RADIUS server: Provides the RADIUS-based authentication service to remote clients. Figure 15- 1 shows the RADIUS server installed with the FS-SAM program.

iPortal Webauth process:

1. Before authentication, the NAS intercepts all HTTP requests from a client and redirects these requests to the iPortal server. Thereafter, an authentication page is displayed on the browser.
2. During authentication, the client enters information, for example, username, password, and verification code, on the Webauth URL to interact with the iPortal server (NAS).
3. The NAS initiates authentication to the RADIUS server and displays the authentication result (success or failure) to the client on a page.

Client logout process:

1. The NAS gets a client offline after the **Logout** button on the Web page is clicked.
2. The NAS gets a client offline with traffic lower than the threshold based on the parameters of user online traffic detection.
3. When the RADIUS server forces a client offline based on a certain policy, the NAS pushes a logout page to the client.

Related Configuration

➘ Configuring the iPortal Webauth Template

By default, the iPortal Webauth template is not configured.

Run the **web-auth template iportal** command in global configuration mode to create an iPortal Webauth template.

The template is used to configure authentication-related parameters on the iPortal server.

Customizing a Page Suite

By default, the factory file package is used.

Run the **page-suite** command in template configuration mode to specify the use of a page suite.

Before you specify the use of a page suite, download it to the flash memory.

Configuring an Advertisement URL

By default, no advertisement URL is configured.

Run the **popup** *url* command in template configuration mode to configure the advertisement URL.

Advertisement URLs allow the push of specified pages to clients.

Specifying the Advertisement Mode

The default advertisement mode is post-login mode.

Run the **popup mode** command in template configuration mode to specify the iPortal Webauth advertisement mode including pre-login mode and post-login mode.

Specifying the Webauth Binding Mode

The default Webauth binding mode is IP-MAC binding mode.

Run the **bindmode** command in template configuration mode to specify the Webauth binding mode.

In Web authentication on layer-3 networks, the source MAC address in a packet is changed after the packet is routed. In such case, configure the IP-only binding mode.

Enabling FS iPortal Web Authentication

By default, FS iPortal Web Authentication is disabled.

Run the **web-auth enable** command in interface configuration mode to enable FS iPortal Web Authentication on the client-connected ports.

After Web authentication is enabled, the unauthenticated clients connecting to a port will be redirected to the Webauth URL.

Enabling AAA

By default, AAA is disabled.

Run the **aaa new-model** command in global configuration mode to enable AAA.

Configuring the RADIUS-Server Host and Communication Key

By default, the RADIUS-server host and communication key are not configured.

Run the **radius-server host** command in global configuration mode to configure the RADIUS-server host and communication key.

The RADIUS-server host in Web authentication is responsible for authenticating users.

Configuring an AAA Method List for FS iPortal Web Authentication

By default, no AAA method list is configured for FS iPortal Web Authentication.

Run the **aaa authentication iportal** command in global configuration mode to configure an AAA method list for FS iPortal Web Authentication.

The AAA authentication method list is used for interaction during the Webauth process.

Configuring an AAA Method List for FS iPortal Web Accounting

By default, no AAA method list is configured for FS iPortal Web Accounting.

Run the **aaa accounting network** command in global configuration mode to configure an AAA method list for FS iPortal Web Accounting.

The AAA accounting method list is used for accounting interaction during the Webauth process.

Specifying an AAA Method List

The default AAA method list is used if no list is specified.

Run the **authentication** command in template configuration mode to specify an AAA method list.

The AAA method list is specified to send authentication requests to AAA.

Specifying an AAA Accounting Method List

The default AAA accounting method list is used if no list is specified.

Run the **accounting** command in template configuration mode to specify an AAA accounting method list.

The AAA accounting method list is specified to send accounting requests to AAA.

15.4 Configuration

Configuration	Description and Command	
Configuring FS First-Generation Web Authentication	(Mandatory) It is used to set the basic parameters of FS First-Generation Web Authentication.	
	web-auth template eportalv1	Configures the first-generation Webauth template.
	ip {*ip-address* }	Configures the IP address of the portal server.
	url { *url-string* }	Configures the Webauth URL of the portal server.
	web-auth portal key { *key-string* }	Configures the Webauth communication key.
	snmp-server community { *community-string* } **rw**	Configures the SNMP-server community string.
	snmp-server host { *ip-address* } **inform version** 2c { *community-string* } **web-auth**	Configures the SNMP-server host.
	web-auth enable	Enables FS First-Generation Web Authentication on an interface.

Configuration	Description and Command	
Configuring FS Second-Generation Web Authentication	(Mandatory) It is used to set the basic parameters of FS Second-Generation Web Authentication.	
	aaa new-model	Enables AAA.
	radius-server host {*ip-address*}[**auth-port** *port-number*] [**acct-port** *port-number*] **key** {*string*}	Configures the RADIUS-server host and communication key.
	aaa authentication web-auth { **default** | *list-name* } *method1* [*method2*...]	Configures an AAA method list for Web authentication. (RADIUS authentication is implemented.)
	aaa accounting network { **default** | *list-name* } **start-stop** *method1* [*method2*...]	Configures an AAA method list for Web Accounting. (RADIUS accounting is implemented.)
	web-auth template{**eportalv2** |*portal-name***v2**}	Configures a second-generation Webauth template.
	ip {*ip-address* }	Configures the IP address of the portal server.
	url { *url-string* }	Configures the Webauth URL of the portal server.
	web-auth portal key { *key-string* }	Configures the Webauth communication key.
	web-auth enable	Enables FS Second-Generation Web Authentication on an interface.
Configuring FS iPortal Web Authentication	(Mandatory) It is used to set the basic parameters of FS iPortal Web authentication.	
	aaa new-model	Enables AAA.
	radius-server host { *ip-address* } [**auth-port** *port-number*] [**acct-port** *port-number*] **key** { *string* }	Configures the RADIUS-server host and communication key.
	aaa authentication iportal { **default** | *list-name* } *method1* [*method2*...]	Configures an AAA method list for FS iPortal Web Authentication. (RADIUS authentication is implemented.)
	aaa accounting network { **default** | *list-name* } **start-stop** *method1* [*method2*...]	Configures an AAA method list for FS iPortal Web Accounting. (RADIUS accounting is implemented.)
	web-auth template iportal	Configures the iPortal Web-auth template.
	web-auth enable	Enables FS iPortal Web Authentication on an interface.
Specifying the Webauth Binding Mode	(Optional) It is used to specify the entry binding mode in template configuration mode.	

Configuration	Description and Command	
	bindmode {ip-mac-mode | ip-only-mode}	Specifies the template binding mode.
Customizing a Page Suite	(Optional) It is used to configure the page suite used by FS iPortal Web Authentication for a template.	
	page-suite *file-name*	Customizes a page suite for FS iPortal Web Authentication.
Specifying the Advertisement Mode	(Optional) It is used to specify the iPortal Webauth advertisement mode in template configuration mode.	
	popup-mode [login-popup | online-popup]	Specifies the iPortal Webauth advertisement mode.
Configuring the Redirection HTTP Port	(Optional) It is used to configure the TCP interception port for redirection, so that the packets on the specified port can be redirected when interception is enabled.	
	http redirect port { *port-num* }	Configures the redirection TCP port.
Configuring Rate Limit Webauth Logging	(Optional) It is used to configure the syslog function in Web authentication.	
	web-auth logging enable {*num* }	Configures the rate limit Webauth logging.
Configuring the Maximum Number of HTTP Sessions for Unauthenticated Clients	(Optional) It is used to adjust the HTTP session limit. The limit value needs to be increased when there are many sessions in the background.	
	http redirect session-limit { *session-num* } [**port** { *port-session-num* }]	Configures the maximum number of HTTP sessions for unauthenticated clients.
Configuring the HTTP Redirection Timeout	(Optional) It is used to modify the timeout period for redirection connections. The timeout needs to be increased to complete redirection when the network condition is bad.	
	http redirect timeout{ *seconds* }	Configures the HTTP redirection timeout.
Configuring the Straight-Through ARP Resource Range	(Optional) It is used to permit the ARP of the specified addresses to pass. The gateway ARP must be permitted to pass when ARP check is enabled.	
	http redirect direct-arp { *ip-address* [*ip-mask*] }	Configures the straight-through ARP resource.
Configuring an Authentication-Exempted Address Range	(Optional) It is used to exempt clients from authentication when accessing the Internet.	
	web-auth direct-host { *ip-address* [i*p-mask*] [**arp**] } [**port** *interface-name* }	Configures the range of the IP or MAC addresses of clients free from authentication.

Configuration	Description and Command	
Configuring the Interval for Updating Online User Information	(Optional) It is used to configure the interval for updating online user information.	
	web-auth update-interval *{ seconds }*	Configures the interval for updating online user information.
Configuring Portal Detection	(Optional) It is used to detect the availability of the portal server. If it is not available, the services are switched to the standby portal server. This function must be used together with portal standby function.	
	web-auth portal-check [**interval** *intsec* [**timeout** *tosec]* [**retransmit** retries]	Configures the portal server detection interval, timeout period, and timeout retransmission times.
Configuring a Whitelist and Blacklist	(Optional) It is used to configure a blacklist to prevent authenticated clients from accessing some network resources, and a whitelist to allow unauthenticated clients to access some network resources.	
	web-auth acl{black-ip *ip*|**black-port** *port*|**black-url** *name*|**white-url** *name*}	Configures a whitelist and blacklist.
Configuring the Default Webauth Template	(Optional) It is used to configure the authentication methods applicable to EG products.	
	web-auth webauth-type {internal | external *name* **}**	
Configuring the Portal Communication Port	(Optional) It is used to configure the port (source port) used for the communication between the NAS and portal server.	
	ip portal source-interface *interface-type interface-num*	Specifies the port used for the communication between the NAS and portal server.
Enabling NAT for FS iPortal Web Authentication	(Optional) It is used to configure FS iPortal Web Authentication to support network address translation (NAT).	
	iportal nat enable	Enables NAT for FS iPortal Web Authentication.
Configuring the iPortal HTTP Retransmission Times	(Optional) It is used to configure the iPortal HTTP retransmission times.	
	iportal retransmit *count*	Configures the iPortal HTTP retransmission times.
Configuring Service Selection in FS iPortal Web Authentication	(Optional) It is used to configure the service type used by FS iPortal Web Authentication.	
	iportal service [**internet** *internet-name*] [**local** *local-name*]	Configures the service type used by FS iPortal Web Authentication.

Configuration	Description and Command	
Configuring the User UA Field in FS iPortal Web Authentication	(Optional) It is used to configure the name of the STA mapped to the user UA field.	
	iportal user-agent *ua-name* **type mobile** *ua-string*	Configures the name of the STA mapped to the user UA field.

15.4.1 Configuring FS First-Generation Web Authentication

Configuration Effect

Redirect unauthenticated clients to the Webauth URL to perform authentication.

Notes

N/A

Configuration Steps

Configuring the Portal Server

- (Mandatory)To enable Web authentication successfully, you must configure and apply the portal server.
- When the NAS or convergence device finds an unauthenticated client attempting to access network resources through HTTP, it redirects the access request to the specified Webauth URL, where the client can initiate authentication to the portal server. If the IP address of the portal server is configured as a free network resource, unauthenticated clients can directly visit this IP address through HTTP.

Configuring the Communication Key Between the NAS and Portal Server

- (Mandatory) To enable Web authentication successfully, you must configure the key used for the communication between the NAS or convergence device and portal server.
- When the NAS finds an unauthenticated client attempting to access network resources, it redirects the client to the specified Webauth URL, where the client can initiate authentication to the portal server. During the authentication process, the communication key is used to encrypt some data exchanged between the NAS and portal server to improve security.

Setting the SNMP Parameters Between the NAS and Portal Server

- (Mandatory) To enable Web authentication successfully, you must set the SNMP network management parameters used for the communication between the NAS and portal server.
- The NAS or convergence device and portal server jointly manage authenticated clients through SNMP/MIB. A table of authenticated clients is managed by MIB on the NAS. The portal server is able to access the MIB to obtain client statistics so as to control client login and logout. When a client logs out, the NAS or convergence device will inform the portal server by Webauth Inform packets.

Enabling FS First-Generation Web Authentication on an Interface

- Mandatory.

- When FS First-Generation Web Authentication is enabled in interface configuration mode, Web authentication is not enabled on any port by default. The users connecting to the port do not need to perform Web authentication.

Verification

- Check whether unauthenticated clients are required to perform authentication.
- Check whether authenticated clients can access the Internet normally.

Related Commands

Configuring the First-Generation Webauth Template

Command	**web-auth template eportalv1**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	**eportalv1** is the default template of FS First-Generation Web Authentication.

Configuring the IP Address of the Portal Server

Command	**ip** {*ip-address*}
Parameter Description	Indicates the IP address of the portal server.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuring the Webauth URL of the Portal Server

Command	**url** {*url-string*}
Parameter Description	*url-string*: Indicates the Webauth URL of the portal server.
Command Mode	Webauth template configuration mode
Usage Guide	The URL starts with **http://** or **https://**.

Configuring the Format of the Webauth URL

Command	**fmt** { **ace** | **FS** }
Parameter Description	Indicates the format of the Webauth URL.
Command Mode	Webauth template configuration mode
Usage Guide	ACE association is supported when **fmt** is set to **ace**.

Specifying the Webauth Binding Mode

Command	**bindmode {ip-only-l3mode}**
Parameter Description	Indicates the Webauth binding mode.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Specifying the Redirection Method

Command	**redirect** { **http** | **js** }
Parameter Description	Indicates the encapsulation format of redirected packets.
Command Mode	Webauth template configuration mode
Usage Guide	For JavaScript-incapable Apps, you need to specify the HTTP encapsulation format to trigger redirection.

Configuring the Webauth Communication Key

Command	**web-auth portal key** {*key-string*}
Parameter Description	*key-string:* Indicates the Webauth communication key used for the communication between the NAS and portal server. The key contains up to 255 characters.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the SNMP-Server Community String

Command	**snmp-server community** {*community-string*}**rw**
Parameter Description	*community-string*: Indicates the community string. **rw**: Must be set to **rw** to support the read and write operations as the Set operation on MIB is required.
Command Mode	Global configuration mode
Usage Guide	The SNMP-server community string is used by the portal server to manage the online clients on the NAS or convergence device.

Configuring the SNMP-Server Host

Command	**snmp-server host** {*ip-address*} **inform version 2c** {*community-string*} **web-auth**
Parameter Description	*ip-address*: Indicates the IP address of the SNMP-server host, that is, the portal server. *community-string*: Configures the community string used to send an SNMP Inform message.
Command Mode	Global configuration mode
Usage Guide	Configure the SNMP-server host to receive Webauth messages, including the type, version, community string, and other parameters. **inform:** Enables the SNMP Inform function. The NAS or convergence device will send a message

	to the portal server when a client logs out. The message type is set to Inform instead of Trap to avoid message loss. **version 2c**: Indicates SNMPv2 for SNMP Inform is not supported in all SNMP versions excluding SNMPv1. **web-auth**: Indicates the preceding parameters to be used for Web authentication. For details regarding SNMP configuration and others, see the *Configuring SNMP*. The SNMP parameter **version 2c**listed here is aimed at SNMPv2. SNMPv3 is recommended if higher security is required for the SNMP communication between the NAS and portal server. To use SNMPv3, change **SNMP Community** to **SNMP User**, **version 2c** to **SNMPv3**, and set SNMPv3-related security parameters. For details, see the *Configuring SNMP*.

Enabling the Webauth Trap/Inform Function

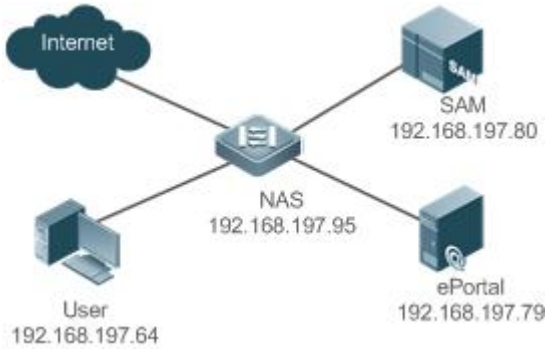
Command	snmp-server enable traps web-auth
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure the NAS or convergence device to send Webauth Trap and Inform messages externally. web-auth: Indicates Web authentication messages.

Enabling FS First-Generation Web Authentication on an Interface

Command	web-auth enable
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuring FS First-Generation Web Authentication

Scenario Figure 15-3	
Configuratio	● On the NAS, configure the IP address of the ePortal server and the key (FS) used for

n Steps	communicating with the ePortal server. ● Configure the Webauth URL on the NAS. ● Set the SNMP network management parameters (community string: public) used for the communication between the NAS and ePortal server. ● Enable Web authentication on ports GigabitEthernet 0/2 and GigabitEthernet 0/3 on the NAS.
	FS# config Enter configuration commands, one per line. End with CNTL/Z. FS(config)#web-auth template eportalv1 FS(config.tmplt.eportalv1)#ip 192.168.197.79 FS(config.tmplt.eportalv1)#exit FS(config)# web-auth portal key FS
	FS(config)# web-auth template eportalv1 FS(config.tmplt.eportalv1)#url http://192.168.197.79:8080/eportal/index.jsp FS(config.tmplt.eportalv1)#exit
	FS(config)# snmp-server community public rw FS(config)# snmp-server enable traps web-auth FS(config)# snmp-server host 192.168.197.79 inform version 2c public web-auth FS(config)# exit
	FS(config)# interface range GigabitEthernet 0/2-3 FS(config-if-range)# web-auth enable FS(config-if-range)# exit
Verification	● Check whether Web authentication is configured successfully.

	FS(config)#show running-config
	...
	snmp-server host 192.168.197.79 inform version 2c public web-auth
	snmp-server enable traps web-auth
	snmp-server community public rw
	...
	web-auth template eportalv1
	  ip 192.168.197.79
	  url http://192.168.197.79:8080/eportal/index.jsp
	!

	web-auth portal key FS ... interface GigabitEthernet 0/2 web-auth enable ! interface GigabitEthernet 0/3 web-auth enable
	FS#show web-auth control Port Control Server Name Online User Count ---------- -------- ---------- ---------- ... GigabitEthernet 0/2On eportalv1 0 GigabitEthernet 0/3On eportalv1 0 ...
	FS#show web-auth template Webauth Template Settings: ---------- Name: eportalv1 Url: http://17.17.1.21:8080/eportal/index.jsp Ip: 17.17.1.21 BindMode: ip-mac-mode Type: v1 .....

Common Errors

- The SNMP parameters used for the communication between the portal server and NAS are configured incorrectly, causing authentication failures.
- When Web authentication is used in conjunction with VRRP, run the snmp-server trap-source ip command to specify the VRRP address; otherwise, the portal server cannot process Trap packets correctly.

15.4.2 Configuring FS Second-Generation Web Authentication

Configuration Effect

Redirect unauthenticated clients to the Webauth URL to perform authentication. IPv6 is supported.

Notes

- FS Second-Generation Web Authentication complies with the CMCC WLAN Service Portal Specification. Furthermore, it is extended to support FS portal server. Perform compatible configuration based on the server performance in actual deployment. For details, see the subsequent chapter.
- The cmcc-normal and cmcc-ext1 parameters in the fmt command support only IPv4. If IPv6 is used, the configuration of the portal server is invalid.

Configuration Steps

Enabling AAA

- (Mandatory) To enable FS Second-Generation Web Authentication, you must enable AAA.
- The NAS is responsible for initiating authentication to the portal server through AAA in FS Second-Generation Web Authentication.

Configuring the RADIUS-Server Host and Communication Key

- (Mandatory) To enable FS Second-Generation Web Authentication, you must configure the RADIUS server.
- Clients' account information is stored on the RADIUS server. The NAS needs to connect to the RADIUS server to validate a client.

Configuring an AAA Method List for Web Authentication

- (Mandatory) To enable FS Second-Generation Web Authentication, you must configure an AAA authentication method list.
- An AAA authentication method list associates Web authentication requests with the RADIUS server. The NAS selects an authentication method and server based on the method list.

Configuring an AAA Method List for Web Accounting

- (Mandatory) To enable FS Second-Generation Web Authentication, you must configure an AAA method list for Web accounting.
- An accounting method list is used to associate an accounting method and server. In Web authentication, accounting is implemented to record client fees.

Configuring the Portal Server

- (Mandatory) To enable FS Second-Generation Web Authentication, you must configure and apply the portal server.
- When the NAS or convergence device finds an unauthenticated client attempting to access network resources through HTTP, it redirects the access request to the specified Webauth URL, where the client can initiate authentication to the portal server. If the IP address of the portal server is configured as a free network resource, unauthenticated clients can directly visit this IP address through HTTP.

Configuring the Communication Key Between the NAS and Portal Server

- (Mandatory) To enable FS Second-Generation Web Authentication, you must configure the key used for the communication between the NAS or convergence device and portal server.
- When the NAS finds an unauthenticated client attempting to access network resources, it redirects the client to the specified Webauth URL, where the client can initiate authentication to the portal server. During the authentication process, the communication key is used to encrypt some data exchanged between the NAS and portal server to improve security.

Configuring the Portal Server in Global or Interface Configuration Mode

- (Mandatory) To enable FS Second-Generation Web Authentication, you must specify the use of the second generation portal server in global or interface configuration mode.
- The NAS first selects the portal server in interface configuration mode. If such a portal server does not exist, the NAS selects the portal server in global configuration mode. If such a portal server does not exist, eportalv1 is used by default. The NAS redirects users to the selected portal server.

Enabling FS Second-Generation Web Authentication on an Interface

- Mandatory.
- When FS Second-Generation Web Authentication is enabled in interface configuration mode, Web authentication is not enabled on any port by default. The users connecting to the port do not need to perform Web authentication.

Verification

- Check whether unauthenticated clients are required to perform authentication.
- Check whether authenticated clients can access the Internet normally.

Related Commands

Enabling AAA

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	You can configure the AAA authentication and accounting method lists only after AAA is enabled.

Configuring the RADIUS-Server Host and Communication Key

Command	**radius-server host** {*ip-address*} [**auth-port***port-number1*] [**acct-port** *port-number 2*] **key** {*string*}
Parameter Description	*ip-address*: Indicates the IP address of the RADIUS server host. *port-number1:* Indicates the authentication port. *port-number2:* Indicates the accounting port. *string*: Indicates the key string.
Command Mode	Global configuration mode

Usage Guide	By default, the authentication port number is 1812, and the accounting port number is 1813.

Configuring an AAA Method List for Web Authentication

Command	**aaa authentication web-auth** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	*list-name*: Creates a method list. *method1*: Configures method 1. *method2*: Configures method 2.
Command Mode	Global configuration mode
Usage Guide	FS Second-Generation Web Authentication adopts the RADIUS authentication method.

Configuring an AAA Method List for Web Accounting

Command	**aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Parameter Description	*list-name*: Creates a method list. *method1*: Configures method 1. *method2*: Configures method 2.
Command Mode	Global configuration mode
Usage Guide	FS Second-Generation Web Authentication adopts the RADIUS accounting method.

Configuring the Second-Generation Webauth Template

Command	**web-auth template**{**eportalv2 |** *portal-name* **v2**}
Parameter Description	*portal-name*: Indicates the customized portal server name.
Command Mode	Global configuration mode
Usage Guide	**eportalv2** indicates the default template of FS Second-Generation Web Authentication.

Configuring the IP Address of the Portal Server

Command	**ip** { *ip-address* }
Parameter Description	Indicates the IP address of the portal server.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuring the Webauth URL of the Portal Server

Command	**url** { *url-string* }
Parameter Description	Indicates the Webauth URL of the portal server.
Command Mode	Webauth template configuration mode
Usage Guide	The URL starts with **http://** or **https://**.

Configuring the Format of the Webauth URL

Command	**fmt { cmcc-ext1 | cmcc-ext2 | cmcc-mtx | cmcc-normal | cmcc-ext3 | FS | custom}**
Parameter Description	Indicates the format of the Webauth URL.
Command Mode	Webauth template configuration mode
Usage Guide	The **cmcc-normal** and **cmcc-ext1** parameters in the **fmt** command support only IPv4. If IPv6 is used, the configuration of the portal server is invalid. The **cmcc-ext2** is supported for Liaoning CMCC. When **fmt** is set to **cmcc-mtx**, the URL format of mobile AC vendors is supported. When **fmt** is set to **cmcc- ext3**, the URL format of Ningbo/Jiaxing mobile AC vendors is supported. **FS** is the default format. The **custom** format is defined by users.

Specifying the Template Binding Mode

Command	**bindmode {ip-only-l3mode}**
Parameter Description	Indicates the template binding mode
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Specifying the Encapsulation Format of the Webauth URL

Command	**redirect { http | js }**
Parameter Description	Indicates the encapsulation format of redirected packets.
Command Mode	Webauth template configuration mode
Usage Guide	For JavaScript-incapable Apps, you need to specify the HTTP encapsulation format to trigger redirection.

Configuring the Webauth Communication Key

Command	**web-auth portal key** { *key-string* }
Parameter Description	*key-string*: Indicates the Webauth communication key used for the communication between the NAS and portal server. The key contains up to 255 characters.
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling FS Second-Generation Web Authentication on an Interface

Command	**web-auth enable**
Parameter Description	Indicates a Webauth template.

Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuring FS Second-Generation Web Authentication

Scenario Figure 15-4	
Configuration Steps	● Enable AAA on the NAS. ● Configure the RADIUS-server host and communication key on the NAS. ● Configure the default AAA method lists for Web authentication and accounting on the NAS. ● Configure the IP address of the portal server and the Webauth communication key (FS) used for communicating with the portal server on the NAS. ● Configure the Webauth URL on the NAS. ● Configure FS Second-Generation Web Authentication in global configuration mode on the NAS. ● Enable Web authentication on ports GigabitEthernet 0/2 and GigabitEthernet 0/3 on the NAS.
	FS#configure Enter configuration commands, one per line. End with CNTL/Z. FS(config)#aaa new-model
	FS(config)#radius-server host 192.168.197.79 key FS
	FS(config)#aaa authentication web-auth default group radius FS(config)#aaa accounting network default start-stop group radius
	FS(config)#web-auth template eportalv2 FS(config.tmplt.eportalv2)#ip 192.168.197.79 FS(config.tmplt.eportalv2)#exit FS(config)#web-auth portal key FS
	FS(config)# web-auth template eportalv2 FS(config.tmplt.eportalv2)#url http://192.168.197.79:8080/eportal/index.jsp

```
FS(config.tmplt.eportalv2)#exit
```

```
FS(config)# interface range GigabitEthernet 0/2-3
FS(config-if-range)# web-auth enable eportalv2
FS(config-if-range)# exit
```

Verification

- Check whether Web authentication is configured successfully.

```
FS(config)#show running-config
...
aaa new-model
aaa authentication web-auth default group radius
aaa accounting network default start-stop group radius
...
radius-server host 192.168.197.79 key FS
...
web-auth template eportalv2
 ip 192.168.197.79
 url http://192.168.197.79:8080/eportal/index.jsp
!
web-auth portal key FS
...
interface GigabitEthernet 0/2
 web-auth enable eportalv2
!
interface GigabitEthernet 0/3
 web-auth enable eportalv2
```

```
FS#show web-auth control
 Port                          Control   Server Name              Online User Count
 ------------------------ -------- -------------------- -----------------
...
GigabitEthernet 0/2          On        eportalv2                0
GigabitEthernet 0/3          On        eportalv2                0
...
```

```
FS#show web-auth template
```

```
Webauth Template Settings:
-------------------------------------------------------
  Name:        eportalv2
  Url:         http://17.17.1.21:8080/eportal/index.jsp
  Ip:          17.17.1.21
  BindMode:    ip-mac-mode
  Type:        v2
  Port:        50100
State:       Active
  Acctmlist: default
  Authmlist: default
...
```

Common Errors

- The communication key between the portal server and NAS is configured incorrectly or only on the portal server or NAS, causing authentication errors.
- The communication parameters of the RADIUS server and NAS are set incorrectly, causing authentication errors.
- The portal server does not support the *CMCC WLAN Service Portal Specification*, causing compatibility failure.

15.4.3 Configuring FS iPortal Web Authentication

Configuration Effect

Redirect unauthenticated clients to the Webauth URL to perform authentication. No external portal server is required.

Notes

- Some devices, such asAP110, do not have a built-in page suite. You need to import a page suite before use. For details about the page suite support on a product, see the corresponding product description.
- FS iPortal Web Authentication is configured on EG devices in global configuration mode.
- To configure a customized page suite, the configuration must comply with the relevant specification.

Configuration Steps

↘ **Enabling AAA**

- Mandatory.
- The iPortal NAS is responsible for initiating authentication to the portal server through AAA in FS iPortal Web authentication.

Configuring the RADIUS-Server Host and Communication Key

- (Mandatory) To enable FS iPortal Web Authentication, you must configure the RADIUS-server host.
- Clients' account information is stored on the RADIUS server. The NAS needs to connect to the RADIUS server to validate a client.

Configuring an AAA Method List for FS iPortal Web Authentication

- (Mandatory) To enable FS iPortal Web Authentication, you must configure an AAA method list for FS iPortal Web Authentication.
- An AAA authentication method list associates Web authentication requests with the RADIUS server. The NAS selects an authentication method and server based on the method list.

Configuring an AAA Method List for FS iPortal Web Accounting

- (Optional) Some servers require that authentication and accounting be enabled. Configure Web accounting based on the characteristics of the server in use.
- An AAA accounting method list associates an accounting method and server. In Web authentication, accounting is implemented to record client fees.

Configuring the iPortal Webauth Template

- Mandatory.
- If any non-default authentication and accounting method lists are configured, you need to specify the name of a method list in template configuration mode; otherwise, the default method list is used.

Enabling FS iPortal Web Authentication Globally or on an Interface

- Mandatory.

Verification

- Check whether unauthenticated clients are redirected to the Webauth URL to perform authentication, and the Webauth URL displayed is that in the page suite.
- Check whether authenticated clients can access the Internet normally.

Related Commands

Enabling AAA

Command	aaa new-model
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	You can configure the AAA authentication and accounting method lists only after AAA is enabled.

Configuring the RADIUS-Server Host and Communication Key

Command	**radius-server host** { *ip-address* } [**auth-port***port-number1*] [**acct-port** *port-number 2*] **key** { *string* }
Parameter Description	*ip-address*: Indicates the IP address of the RADIUS-server host. *port-number1:* Indicates the authentication port. *port-number2:* Indicates the accounting port. *string*: Indicates the key string.
Command Mode	Global configuration mode
Usage Guide	By default, the authentication port number is 1812, and the accounting port number is 1813.

Configuring an AAA Method List for FS iPortal Web Authentication

Command	**aaa authentication iportal** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	*list-name*: Creates a method list. *method1*: Indicates method 1. *method2*: Indicates method 2.
Command Mode	Global configuration mode
Usage Guide	The specified AAA method should exist in the AAA configuration.

Configuring an AAA Method List for Web Accounting

Command	**aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Parameter Description	*list-name*: Creates a method list. *method1*: Indicates method 1. *method2*: Indicates method 2.
Command Mode	Global configuration mode
Usage Guide	The specified AAA method should exist in the AAA configuration.

Configuring the iPortal Webauth Template

Command	**web-auth template iportal**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Specifying the Pre-login Advertisement Mode

Command	**login-popup**{ *url-string* }
Parameter Description	Indicates the advertisement URL.
Command Mode	Webauth template configuration mode
Usage Guide	The URL starts with **http://** or **https://**.

Specifying the Post-login Advertisement Mode

Command	**online-popup** {url-string}
Parameter Description	Indicates the advertisement URL.
Command Mode	Webauth template configuration mode
Usage Guide	The URL starts with **http://** or **https://**.

Customizing a Page Suite

Command	**page-suit**{*filename*}
Parameter Description	Indicates the file name of a page suite.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuring the iPortal Advertisement Interval

Command	**time-interval** {*hour*}
Parameter Description	Indicates the advertisement interval.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Enabling FS iPortal Web Authentication on an Interface

Command	**web-auth enable**
Parameter Description	Indicates the customized template name.
Command Mode	Interface configuration mode or global configuration mode
Usage Guide	N/A

Configuration Example

Configuring FS iPortal Web Authentication

Configuration Steps	• Enable AAA on the NAS. • Configure the RADIUS-server host and communication key on the NAS. • Configure the default AAA authentication and accounting method lists on the NAS. • Configure the global use of the iPortal server on the NAS. • Enable Web authentication on ports GigabitEthernet 0/2 and GigabitEthernet 0/3 on the NAS.
	FS#configure

	Enter configuration commands, one per line. End with CNTL/Z. FS(config)#aaa new-model
	FS(config)#radius-server host 192.168.197.79 key FS
	FS(config)#aaa authentication iportal default group radius FS(config)#aaa accounting network default start-stop group radius
	FS(config)#web-auth template iportal
	FS(config.tmplt.iportal)#exit
	FS(config)# interface range GigabitEthernet 0/2-3 FS(config-if-range)# web-auth enable iportal FS(config-if-range)# exit
Verification	● Check whether FS iPortal Web Authentication is configured successfully.

	FS(config)#show running-config
	...
	aaa new-model
	aaa authentication web-auth default group radius
	aaa accounting network default start-stop group radius
	...
	radius-server host 192.168.197.79 key fs
	...
	web-auth template iportal
	!
	...
	interface GigabitEthernet 0/2
	  web-auth enable iportal
	!
	interface GigabitEthernet 0/3
	  web-auth enable iportal

	FS#show web-auth control
	  Port Control Server Name Online User Count
	  ---------- -------- ---------- ----------
	...

	GigabitEthernet 0/2 On iportal 0 GigabitEthernet 0/3 On iportal 0 ...
	FS#show web-auth template Webauth Template Settings: ---------- Name: iportal Page-suit: default BindMode: ip-mac-mode Type: Intral Portal Advertising: null Advertising mode : online-popup Acctmlist: default Authmlist: default ...

Common Errors

- The preparation of a page suite does not comply with the relevant specification.
- A page suite is specified, but is not downloaded to the flash memory or the specified directory.

15.4.4 Specifying the Webauth Binding Mode

Configuration Effect

- When a user goes online, the user's entry needs to be written to a forwarding rule. The forwarding rule mapping method can be modified by specifying different binding modes, which further affects the Internet access rules applied to users. In IP-only mode, all the packets carrying the specified IP address are permitted to pass, and the STAs who send the packets can access the Internet. In IP+MAC mode, only the packets carrying both the specified IP address and MAC address are permitted to pass, and the STAs who send the packets can access the Internet.

Notes

- In Layer-3 authentication, the MAC addresses visible to the NAS are the gateway addresses of STAs. Because these MAC addresses are not accurate, the IP-only mode should be used.

Configuration Steps

- (Optional) The default Webauth binding mode is IP+MAC.

- Determine a binding mode based on the accuracy of user information obtained by the NAS. When the IP and MAC addresses of STAs are accurate (in L2 authentication, for example), IP+MAC is recommended. When the IP and MAC addresses are not accurate, select IP-only.

Verification

- Change the binding mode to IP-only.
- Simulate the scenario where a user performs authentication to access the Internet.
- Modify the MAC address of the user, or use a client with the same IP address but a different MAC address to access the Internet.
- Check that the user accesses the Internet normally.

Related Commands

Specifying the Webauth Binding Mode

Command	**bindmode {ip-only-l3mode}**
Parameter Description	**ip-only- l3mode**: Indicates IP-only binding mode.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuration Example

Specifying the Webauth Binding Mode

Configuration Steps	● Set the binding mode to IP-only.
	FS(config.tmplt.eportalv2)#bindmode ip-only-mode
Verification	● Check whether the configuration is successful.
	FS#show web-auth template Webauth Template Settings: ---------- Name: eportalv2 Url: http://17.17.1.21:8080/eportal/index.jsp Ip: 17.17.1.21 BindMode: ip-only-mode Type: v2 Port: 10000 Acctmlist:

Configuration Steps	● Set the binding mode to IP-only.
	FS(config.tmplt.eportalv2)#bindmode ip-only-mode
Verification	● Check whether the configuration is successful.
	Authmlist:

15.4.5 Customizing a Page Suite

Configuration Effect

- Configure a page suite to be used on the iPortal server and add special content or information to the page suite, for example, a logo or notice.

Notes

- A page suite must be downloaded manually to the flash memory of the NAS and saved to the ./portal directory. If the page suite is not saved or is saved to an incorrect directory, page push will fail, causing Web authentication invalid. The default page suite can be used if there are no special requirements.
- For details, see section 15.4.21 "Customizing a Page Suite."

Configuration Steps

- (Optional) By default, the default page suite is used.

Verification

- Configure FS iPortal Web Authentication.
- Download a page suite.
- Specify the page suite.
- Check whether the page suite is applied to the login page.

Related Commands

↘ Customizing a Page Suite

Command	**page-suit** *filename*
Parameter Description	*filename*: Indicates the file name of a page suite.
Command Mode	Webauth template configuration mode
Usage Guide	Download the page suite to be used to the **./porta/zipl** directory of the flash memory in advance.

Configuration Example

↘ Customizing a Page Suite

Configuration Steps	● Customize a page suite.
	FS(config.tmplt.iportal)#page-suitfspage
Verification	● Check whether the configuration is successful.
	FS#show web-auth template Webauth Template Settings: ---------- Name: iportal FS#show web-auth template Webauth Template Settings: ---------- Name: iportal Page-suit: fspage Advertising url: default Advertising mode: online-popup Type: Intral Portal Acctmlist:default Authmlist:default

15.4.6 Configuring the Advertisement Pushing Mode

Configuration Effect

- Optional. Advertisements are pushed before or after authentication.

Notes

- The advertisement URI needs to be configured in advance.
- By default, advertisements are pushed after authentication is successful.
- To ensure that only advertisements are pushed in the case that users are not authenticated, select the advertising function. For details, see the advertising configuration manual.

Configuration Steps

- (Optional) By default, advertisements are pushed after the authentication is successful.

Verification

- Configure embedded portal Web authentication.
- Configure a URL address that can access the Internet.

- When a user accesses the network, check whether a new window is displayed after the authentication is successful and whether information on a page of a specific URI is displayed.

Related Commands

Configuring the Advertisement Pushing Address

Command	**login-popup** *url*
Parameter Description	*url*: Indicates the address pushed before authentication (during login).
Command Mode	Webauth template configuration mode
Usage Guide	
Command	**online-popup** *url*
Parameter Description	*url*: Indicates the address pushed after the authentication is successful.
Command Mode	Webauth template configuration mode
Usage Guide	

Configuration Example

Configuring the Advertisement Pushing Mode

Configuration Steps	• Configure the advertisement pushing mode to advertisement pushing before authentication.
	FS(config.tmplt.iportal)#login-popup http://www.fs.com.cn/ FS(config.tmplt.iportal)#popup mode login-popup
Verification	• Check whether the advertisement pushing mode is configured successfully.
	FS#show web-auth template Webauth Template Settings: ---------- Name: iportal Page-suit: default Advertising url: http://www.fs.com.cn/ Advertising mode: login-popup Type: Intral Portal Acctmlist:default Authmlist:default

15.4.7 Configuring the Redirection HTTP Port

Configuration Effect

- When an STA accesses network resources (for example, the user accesses the Internet using a browser), the STA sends HTTP packets. The NAS or convergence device intercepts these HTTP packets to determine whether the STA is accessing network resources. If the NAS or convergence device detects that the STA is not authenticated, it prevents the STA from accessing network resources and displays an authentication page to the STA. By default, the NAS intercepts the HTTP packets that STAs send to port 80 to determine whether STAs are accessing network resources.
- After a redirection HTTP port is configured, the HTTP requests that STAs send to the specified destination port can be redirected.

Notes

- The commonly used management ports on the NAS or convergence device, such as ports 22, 23 and 53, and ports reserved by the system are not allowed to be configured as the redirection port. All ports except port 80 with numbers smaller than 1000 are seldom used by the HTTP protocol. To avoid a conflict with the well-known TCP port, do not configure a port with a small number as the redirection port unless necessary.

Configuration Steps

- Optional.
- When you configure automatic client acquisition, if you need to enable the NAS to intercept the HTTP packets that STAs send to the specified destination port, configure a redirection HTTP port.

Verification

- Configure an interception port.
- Open the browser of a PC and access the Internet through the port without performing authentication.
- Check whether the access requests are redirected to an authentication page.

Related Commands

Configuring the Redirection HTTP Port

Command	**http redirect port** *port-num*
Parameter Description	*port-num*: Indicates the port number.
Command Mode	Global configuration mode
Usage Guide	A maximum of 10 different destination port numbers can be configured, not including default ports 80 and 443.

Configuration Example

Configuring the Redirection HTTP Port

Configuration Steps	● Configure port 8080 as the redirection HTTP port.
	FS(config)#http redirect port 8080
Verification	● Check whether the configuration is successful.
	FS(config)#show web-auth rdport Rd-Port: 80 443 8080

15.4.8 Configuring Rate Limit Webauth Logging

Configuration Effect

- The Web authentication module sends syslog messages to the administrator to display the information and relevant events of users who perform login/logout. By default, syslog messages are shielded.
- After syslog output rate limiting is configured, syslog messages are sent at a certain rate.

Notes

- When the login/logout rate is high, syslog messages are output frequently, which affects device performance and results in spamming.

Configuration Steps

- Optional.
- Configure syslog output rate limiting when you need to view the syslog messages about user login/logout.

Verification

- Configure logging rate limiting.
- Check whether users log in and out at a certain rate.
- Check that syslog messages are printed out at the limit rate.

Related Commands

↘ Configuring Rate Limit Webauth Logging

Command	**web-auth logging enable** *num*
Parameter Description	*num*: Indicates the syslog output rate (entry/second).
Command Mode	Global configuration mode
Usage Guide	When the syslog output rate is set to **0**, syslog messages are output without limit. The output of syslog messages of the critical level and syslog messages indicating errors is not limited.

Configuration Example

Configuring Rate Limit Webauth Logging

Configuration Steps	● Disable rate limit Webauth Logging.
	FS(config)#web-auth logging enable 0
Verification	● Check whether the configuration is successful.
	FS(config)#show running-config ... web-auth logging enable 0 ...

15.4.9 Configuring the Maximum Number of HTTP Sessions for Unauthenticated Clients

Configuration Effect

- When an unauthenticated user accesses network resources, the user's PC sends requests for HTTP session connection. The NAS or convergence device intercepts the HTTP packets and redirects the user to a Web authentication page. To prevent an unauthenticated user from initiating too many HTTP connection requests and save resources on the NAS, it is necessary to limit the maximum number of HTTP sessions that the unauthenticated user can initiate on the NAS.
- A user occupies an HTTP session when performing authentication, and the other application programs of the user may also occupy HTTP sessions. For this reason, it is recommended that the maximum number of HTTP sessions for an unauthenticated user be not set to 1. By default, each unauthenticated user can initiate 255 HTTP sessions globally, and each port supports up to 300 HTTP sessions initiated by unauthenticated clients.

Notes

- If the authentication page fails to be displayed during Web authentication, the maximum number of HTTP sessions may be reached. When this happens, the user can close the application programs that may occupy HTTP sessions and then perform Web authentication again.

Configuration Steps

- Optional.
- Perform this configuration when you need to change the maximum number of HTTP sessions that each unauthenticated user can initiate and the maximum number of HTTP sessions that unauthenticated clients can initiate on each port.
- Perform this configuration when you configure automatic SU client acquisition.

Verification

- Modify the maximum number of HTTP sessions that an unauthenticated user can initiate.
- Simulate the scenario where an unauthenticated user constructs identical sessions to connect to the NAS continuously.
- Simulate the scenario where the unauthenticated user accesses the Internet using a browser. Check whether the access requests are redirected and the NAS notifies the user that the maximum number of sessions is reached.

Related Commands

Configuring the Maximum Number of HTTP Sessions for Unauthenticated Clients

Command	**http redirect session-limit** { *session-num* }[**port** { *port-session-num* }]
Parameter Description	*session-num*: Indicates the maximum number of HTTP sessions for unauthenticated clients. The value range is 1 to 255. The default value is 255. *port-session-num*: Indicates the maximum number of HTTP sessions on each port for authenticated clients. The value range is 1 to 65,535. The default value is 300.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Maximum Number of HTTP Sessions for Unauthenticated Clients

Configuration Steps	● Set the maximum number of HTTP sessions for unauthenticated clients to 3.
	FS(config)#http redirect session-limit 3
Verification	● Check whether the configuration is successful.
	FS(config)#show web-auth parameter HTTP redirection setting: session-limit: 3 timeout: 3 FS(config)#

15.4.10 Configuring the HTTP Redirection Timeout

Configuration Effect

- Configure the HTTP redirection timeout to maintain redirection connections. When an unauthenticated user tries to access network resources through HTTP, the TCP connection requests sent by the user will be intercepted and re-established with the NAS or convergence device. Then, the NAS or convergence device waits for the HTTP GET/HEAD packets from the user and responds with HTTP redirection packets to close the connection. The redirection timeout is intended to prevent the user from occupying the

TCP connection for a long time without sending GET/HEAD packets. By default, the timeout for maintaining a redirection connection is 3s.

Notes

N/A

Configuration Steps

- Optional.
- Perform this configuration to change the timeout for maintaining redirection connections.

Verification

- Change the timeout period.
- Use a network packet delivery tool to set up a TCP connection.
- View the status of the TCP connection on the NAS. Check whether the TCP connection is closed when the timeout is reached.

Related Commands

Configuring the HTTP Redirection Timeout

Command	**http redirect timeout** { *seconds* }
Parameter Description	*Seconds*: Indicates the timeout for maintaining redirection connections, in the unit of seconds. The value ranges from 1 to 10. The default value is 3s.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the HTTP Redirection Timeout

Configuration Steps	● Set the HTTP redirection timeout to 5s.
	FS(config)#http redirect timeout 5
Verification	● Check whether the configuration is successful.
	FS(config)#show web-auth parameter HTTP redirection setting: session-limit: 255 timeout: 5

15.4.11 Configuring the Straight-Through Network Resources

Configuration Effect

- After Web authentication or 802.1Xauthentication is enabled on a port, the users connecting to the port need to pass Web authentication or 802.1Xauthentication before accessing network resources.
- Perform this configuration to exempt users from authentication when accessing some network resources.
- If a website is configured as a network resource of authentication exemption, all users, including unauthenticated clients, can access the website. By default, authentication exemption is not configured, and unauthenticated clients are not allowed to access network resources.

Notes

- The maximum number of free resources and the maximum number of unauthenticated clients cannot exceed 1000 respectively. The actual number of available resources may be reduced because of other security modules. Therefore, it is recommended that network segments be configured if many addresses need to be set.
- **http redirect direct-site** is used to configure the straight-through URL address for users, and **http redirect** is used to configure the straight-through IP address of the Web authentication server. The addresses configured using the two commands can be accessed without authentication, but they have different usages. It is recommended not to configure the IP address of the Web authentication server by using **http redirect direct-site**.

Configuration Steps

- Optional.
- Run the **http redirect direct-site** command to enable unauthenticated clients to access network resources.

Verification

- Configure the straight-through network resources.
- Check whether unauthenticated clients can access the configured network resources using PCs.

Related Commands

Configuring the Straight-Through Network Resources

Command	**http redirect direct-site** { *ipv4-address* [*ip-mask*] [**arp**] | *mac-address* | range *starip-address endip-address* } [description *description-str*] [group *group-name*]
Parameter Description	*ipv4-address*: Indicates the IPv4 address of the network exempt from authentication. *ip-mask*: Indicates the mask of the IPv4 address of the network exempt from authentication. *mac-address*: Indicates the destination MAC address of the network exempt from authentication. *startip-address*: Indicates the start IP address of consecutive networks exempt from authentication. *endip-address*: Indicates the end IP address of consecutive networks exempt from authentication. *group-name*: Indicates the group to which the network exempt from authentication belongs. *description-str*: Indicates the description of the network exempt from authentication.

Command Mode	Global configuration mode
Usage Guide	To set authentication-exempted ARP resource, use the **http redirect direct-arp** command preferentially.

Configuration Example

Configuring the Straight-Through Network Resources

Configuration Steps	● Configure the straight-through network resources as 192.168.0.0/16.
	FS(config)#http redirect direct-site 192.168.0.0 255.255.0.0
	● Set the range of consecutive networks exempt from authentication to 10.0.0.1-12.0.0.1. FS(config)# http redirect direct-site range 10.0.0.1 12.0.0.1
Verification	● Check whether the configuration is successful.
	FS(config)#show web-auth direct-site Direct sites: Address Mask ARP Binding Group Description --- --- --- --- --- 192.168.0.0 255.255.0.0 Off N/A N/A FS(config)# FS(config)#show web-auth direct-site range Direct site Ranges: 1 Start Address End Address Group Description --- --- --- --- 10.0.0.1 12.0.0.1 N/A N/A FS(config)#

15.4.12 Configuring the Straight-Through ARP Resource Range

Configuration Effect

When ARP check or similar functions are enabled, the ARP learning performed by clients is controlled. As a result, clients cannot learn the ARPs of the gateway and other devices, which affects user experience. You can configure the straight-through ARP resource range to permit the ARP learning packets destined for the specified address to pass.

Notes

- When ARP check is enabled, you need to configure the gateway of the PCs connecting to the Layer-2 access device as a straight-through ARP resource. Note the following point when you perform the configuration:

- When you configure straight-through websites and ARP resources in the same address or network segment, the **http redirect direct-arp** command automatically combines the websites and ARP resources. If no ARP option is specified for the configured websites, an ARP option will be automatically added after the combination.
- When ARP check is enabled, if the outbound addresses of the PCs connecting to the Layer-2 access device are not the gateway address, configure the outbound addresses as straight-through ARP resources. If multiple outbound addresses exist, configure these addresses as straight-through ARP resources.

Configuration Steps

- Optional.
- If ARP check is enabled on the NAS, you must configure the free resources and gateway address as straight-through ARP resources.

Verification

- Configure straight-through ARP resources.
- Clear the ARP cache of the PC of an unauthenticated user. (Run the **arp -d** command in the Windows operating system.)
- Run the **ping** command on the PC to access the straight-through ARP resources.
- View the ARP cache on the PC (run the **arp -a** command in the Windows operating system) and check whether the PC learns the ARP address of the straight-through ARP resources.

Related Commands

Configuring the Straight-Through ARP Resource Range

Command	**http redirect direct-arp** {*ip-address* [*ip-mask*] }
Parameter Description	*ip-address*: Indicates the IP address of free resources. *ip-mask*: Indicates the mask of free resources.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Straight-Through ARP Resource

Configuration Steps	• Configure the straight-through ARP resource as 192.168.0.0/16.
	FS(config)#http redirect direct-arp 192.168.0.0 255.255.0.0
Verification	• Check whether the configuration is successful.
	FS(config)#show web-auth direct-arp

Configuration Steps	● Configure the straight-through ARP resource as 192.168.0.0/16.
	FS(config)#http redirect direct-arp 192.168.0.0 255.255.0.0
Verification	● Check whether the configuration is successful.
	Direct arps: Address Mask --- --- 192.168.0.0 255.255.0.0 FS(config)#

15.4.13 Configuring an Authentication-Exempted Address Range

Configuration Effect

- Exempt users from Web authentication when accessing reachable network resources. By default, no authentication-exempted address range is configured. All users must pass Web authentication before accessing network resources.
- The authentication-exempted address range can be configured as an IP address range or MAC address range.

Notes

N/A

Configuration Steps

- Optional.
- Perform this configuration to allow unauthenticated clients to access network resources.

Verification

- Configure an authentication-exempted user.
- Check whether the user can access the Internet without authentication.

Related Commands

↘ **Configuring an Authentication-Exempted Address Range**

Command	**web-auth direct-host** { *ipv4-address* [i*pv4-mask*] [**arp**] [**port** *interface-name*] | *mac-address* | range *starip-address endip-address* } [description *description-str*] [group *group-name*]
Parameter Description	*ipv4-address*: Indicates the IPv4 address of the user exempt from authentication. *ip-mask*: Indicates the mask of the IPv4 address of the user exempt from authentication. *interface-name*: Indicates the name of the interface on which authentication exemption is enabled.

	mac-address: Indicates the MAC address of the user exempt from authentication. *startip-address*: Indicates the start IP address of consecutive users exempt from authentication. *endip-address*: Indicates the end IP address of consecutive users exempt from authentication. *group-name*: Indicates the group to which the user exempt from authentication belongs. *description-str*: Indicates the description of the user exempt from authentication.
Command Mode	Global configuration mode
Usage Guide	The **arp** field is used to assign pass permissions to ARP packets. This field must be set when ARP check is enabled. After the **port** field is set, authentication exemption takes effect only on the configured interface.

Configuration Example

Configuring an Authentication-Exempted Address Range

Configuration Steps	● Configure an authentication-exempted address range.
	FS (config)# web-auth direct-host 192.168.197.64
	● Set the range of consecutive users exempt from authentication to 10.0.0.1-12.0.0.1. FS(config)# web-auth direct-host range 10.0.0.1 12.0.0.1
Verification	● Check whether the configuration is successful.
	FS(config)#show web-auth direct-host Direct hosts: Address Mask Port ARP Binding Group Description --- --- --- --- --- --- 192.168.197.64 255.255.255.255 Off N/A N/A FS(config)# FS# show web-auth direct-host range Direct host Ranges: 1 Start Address End Address Port Group Description --- --- --- --- --- 10.0.0.1 12.0.0.1 Gi0/2 N/A N/A

15.4.14 Configuring the Interval for Updating Online User Information

Configuration Effect

- The NAS or convergence device maintains and periodically updates the information of online users, including users' online duration, to monitor the usage of network resources. When the online duration threshold is reached, users will be prevented from using network resources.

Notes

- The user information updating interval must be configured as 60 or multiple of 60; otherwise, the system will select the minimum multiple of 60 above and closest to the actual configuration as the interval.

Configuration Steps

- Optional.
- Perform this configuration to allow unauthenticated clients to access network resources.

Verification

- Configure the interval for updating online user information.
- View the information of online users after the update interval has elapsed.

Related Commands

Configuring the Interval for Updating Online User Information

Command	**web-auth update-interval** *{ seconds }*
Parameter Description	*seconds*: Indicates the interval for updating online user information, in the unit of seconds. The value ranges from 30 to 3,600. The default value is 180s.
Command Mode	Global configuration mode
Usage Guide	To restore the default updating interval, run the **no web-auth update-interval** command in global configuration mode.

Configuration Example

Configuring the Interval for Updating Online User Information

Configuration Steps	● Set the interval for updating online user information to 60s.
	FS (config)# web-auth update-interval 60
Verification	● Check whether the configuration is successful.
	FS(config)#show run | include web-auth update-interval web-auth update-interval 60

15.4.15 Configuring a Whitelist and Blacklist

Configuration Effect

- Configure a whitelist to allow unauthenticated clients to access some network resources, and configure a blacklist to prevent authenticated clients from accessing some network resources.
- Blacklists and whitelists are supported based on ports, URLs, and IP addresses.

Notes

- Up to 1,000 blacklists and whitelists can be configured.
- If blacklists and whitelists are configured in the domain name format, the DNS function must be configured on the NAS so that the NAS can resolve IP addresses correctly.
- A domain name can map up to eight IP addresses.

Configuration Steps

- Optional.
- Configure DNS.
- Configure a whitelist and blacklist.

Verification

- Configure a whitelist and blacklist.
- Check whether unauthenticated STAs can access the whitelisted addresses.
- Check whether authenticated STAs cannot access the blacklisted addresses.

Related Commands

Configuring a Whitelist and Blacklist

Command	**web-auth acl{black-ip** *ip*|**black-port** *port*|**black-url** *name*|**white-url** *name***}**
Parameter Description	*ip*: Indicates an IP addresses blacklisted. *port*: Indicates a port numbers blacklisted. *name*: Indicates a URL blacklisted or whitelisted.
Command Mode	Global configuration mode (Blacklists can be configured in WLAN security configuration mode on wireless devices.)
Usage Guide	Configure a whitelist to allow unauthenticated clients to access some network resources, and configure a blacklist to prevent authenticated clients from accessing some network resources.

Configuration Example

Configuring a Whitelist and Blacklist

Configuration Steps	● Configure a whitelist and blacklist.
	FS(config)#web-auth acl black-ip 192.168.1.2 FS(config)#web-auth acl white-url www.fs.com.cn

Verification	● Check whether the configuration is successful.
	FS(config)#show running-config ... web-auth acl black-ip 192.168.1.2 web-auth acl white-url www.fs.com.cn ...

15.4.16 Configuring the Portal Communication Port

Configuration Effect

- Configure the port (source port) used for the communication between the NAS and portal server.

Notes

- Only one port can be configured for the communication between the NAS and portal server.

Configuration Steps

- Configure a port as the portal communication port.

Verification

- After Web authentication is enabled, capture a packet on the portal server during the authentication process and check whether the source IP address of the packet is the IP address of the specified port.

Related Commands

Configuring the Portal Communication Port

Command	**ip portal source-interface** *interface-type interface-num*
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Portal Communication Port

Configuration Steps	● Configure an aggregate port as the portal communication port.
	FS(config)#ip portal source-interface Aggregateport 1
Verification	● Check whether the configuration is successful.

Configuration Steps	● Configure an aggregate port as the portal communication port.
	FS(config)#ip portal source-interface Aggregateport 1
Verification	● Check whether the configuration is successful.
	FS(config)#show running-config ip portal source-interface Aggregateport 1

15.4.17 Enabling NAT for FS iPortal Web Authentication

Configuration Effect

- Configure FS iPortal Web Authentication to support NAT.

Notes

- NAT takes effect only in FS iPortal Web Authentication.

Configuration Steps

Enabling NAT for FS iPortal Web Authentication

- Enable NAT in global configuration mode.

Command	iportal nat enable
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Check whether FS iPortal Web Authentication can be implemented after NAT is enabled.

Configuration Example

Enabling NAT for FS iPortal Web Authentication

Configuration Steps	● Enable NAT for FS iPortal Web Authentication.
	FS(config)#iportal nat enable
Verification	● Check whether the configuration is successful.

Configuration Steps	● Enable NAT for FS iPortal Web Authentication.
	FS(config)#iportal nat enable
Verification	● Check whether the configuration is successful.
	FS(config)#show running-config ... iportal nat enable

15.4.18 Configuring the iPortal HTTP Retransmission Times

Configuration Effect

- Configure the iPortal HTTP retransmission times.

Notes

- The retransmission times configuration takes effect only for the HTTP connections pushed by an iPortal page.

Configuration Steps

Configuring the iPortal HTTP Retransmission Times

- Set a parameter in global configuration mode.

Command	**iportal retransmit** *count*
Parameter Description	*count*: Indicates the retransmission times.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Send an iPortal Web authentication request and disconnect from the network. Check whether the NAS resends an HTTP connection request.

Configuration Example

Configuring the Retransmission Times

Configuration Steps	● Configure the retransmission times.
	FS(config)#iportal retransmit 5

Verification	● Check whether the configuration is successful.
	FS(config)#show running-config ... iportal retransmit 5

15.4.19 Configuring Service Selection in FS iPortal Web Authentication

Configuration Effect

- Configure the service type used by FS iPortal Web Authentication.

Notes

- N/A

Configuration Steps

Configuring the Service Type Used by FS iPortal Web Authentication

- Configure a service type in global configuration mode.

Command	**iportal service [internet** *internet-name*] [**local** *local-name*]
Parameter Description	*internet-name*: Indicates the external service name to be used. *local-name*: Indicates the internal service name to be used.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring a Service Type

Configuration Steps	● Configure a service type.
	FS(config)#iportal service local local-srv
Verification	● Check whether the configuration is successful.
	FS(config)#show running-config ... iportalservice local local-srv

15.4.20 Configuring the User UA Field in FS iPortal Web Authentication

Configuration Effect

- Configure the name of the STA mapped to the user UA field.

Notes

- The function is replaced by STA recognition; therefore, the configuration command is invalid.

Configuration Steps

Configuring the User UA Field in FS iPortal Web Authentication

- Set the UA field in global configuration mode.

Command	**iportal user-agent** *ua-name* **type mobile** *ua-string*
Parameter Description	*ua-name*: Indicates the name mapped to the UA field. *ua-string*: Indicates the content of the UA string.
Command Mode	Global configuration mode
Usage Guide	N/A

15.4.21 Customizing a Page Suite

Configuration Effect

- Customize a webpage to display logos or advertisements in FS iPortal Web Authentication.
- A single page suite supports two page sets to adapt to the screen sizes of STAs, for example, mobile STAs with a small screen.

Notes

- The preparation of a page suite must comply with the relevant specification; otherwise, the customized page suite cannot be used.
- The maximum number of files in a page suite (including the files displayed on PCs and mobile STAs) is 50, and the maximum length of the file name of each page is 32 bytes.
- A new page suite must be downloaded to the ./portal directory and the name must not be the same as that of the default page suite; otherwise, the default page suite will be overwritten.
- Some NASs do not have a default page suite. When FS iPortal Web Authentication is implemented, prepare a page suite in accordance with the relevant specification and import the page suite to the flash memory.

Verification

- Simulate the scenario where an STA connects to the Internet and opens the browser to perform authentication. Check that the customized page is displayed.

Related Commands

Page File Naming Specification

Page File Name (with an Extension)	Usage
login.htm	Login page
online.htm	Online page (which is displayed when users pass authentication)
offline.htm	Offline page
login_mobile.htm	Login page for mobile STAs
online_mobile.htm	Online page for mobile STAs (which is displayed when users pass authentication)
offline_mobile.htm	Offline page for mobile STAs

Login Page Preparation Specification

According to the page file naming specification, the file name of the login page for PCs is login.htm, and that for mobile STAs is login_mobile.htm. The login page content specification is described in the following.

- Form elements

The login page must contain a form, and the form submission method is fixed to POST. The PC login page is used as an example. Assume that the PC login page is stored in the **/portal** directory. The HTML code of the form is as follows (the HTML code of the form of the mobile STA login page is similar):

```
<form method="post" action="/portal/login.htm">
...
</form>
```

The form of the login page must contain the following page elements:

1. (Mandatory) **User name** text box: allows a user to enter the user name. The text box ID is username.
2. (Mandatory) **Password** text box: allows a user to enter the password (which is not displayed in plaintext mode). The text box ID is password.
3. (Mandatory) **Login** button: allows a user to submit a form using the POST method.
4. (Optional) Tab showing an authentication failure cause: The ID of the tab is errormsg. The tab is displayed on the login page to show why the current user fails authentication. When the login page is loaded, an error message request is sent using the GET method, and the request results will be displayed on the errormsg tab. You can configure whether to display the errormsg tab on the login page as required. The following script is used to request the error message content from the server (the script is only one example):

```
< script language="javascript">
//Request the error message content from the server.
function requestErrorMsg() {
    var _errormsg=document.getElementById("errormsg");
```

```
    var script=document.createElement("script");
script.src="errormessage"+location.search;
_errormsg.appendChild(script);
}

//Call the init function when the login page is loaded.
function init() {
……
requestErrorMsg();
}
……
</script>
```

- Form submission

A form is submitted in the format of username=[AAAA]&password=[BBBB]&lang=[CCCC]. The meanings of the fields are described in the following:

[AAAA]: (optional)Indicates the user name that the user enters in the **User name** text box.

[BBBB]: (optional)Indicates the password that the user enters in the **Password** text box.

[CCCC]: (optional) Indicates the language environment. The value **1** indicates Simplified Chinese, and the value **2** indicates English. Other languages are not defined. The default language environment is Simplified Chinese. When English is used, the submitted form must contain the language environment information; otherwise, the content of the errormsg tab is in Chinese.

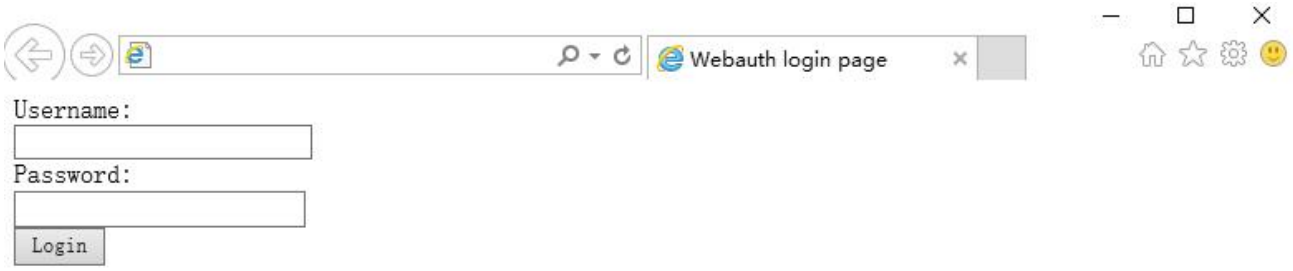
The form of the login page must contain at least the following three input fields (tabs): **username**, **password**, and **Login** button. If the login page provides the Chinese and English language options, the form may also contain the **Language** input field, which is invisible.

The HTML source code of the login page is as follows:

```
<html>
<head>
<title>Web authentication login page</title>
</head>
<script language="javascript">
//Request errormsg. Errormsg is empty and not displayed when a user passes authentication or the login page is loaded for the first time.
    function requestErrorMsg() {
    var _errormsg=document.getElementById("errormsg");
      var script=document.createElement("script");
script.src="errormessage"+location.search;
```

```
_errormsg.appendChild(script);
    }

function init() {
……
requestErrorMsg();
}

//Script that is executed when a user clicks the Login button
function login() {
   document.getElementById('loginForm').action = "./login.htm"+location.search;
      document.getElementById('loginForm').submit();
      window.onbeforeunload = null;
      window.onunload = null;
}
……

</script>
<body onload="init()">
<form method="post" id="loginForm">
User name:<br>
<input type="text" name="username" accesskey="u" size="25" value="" id="usrename">
<br>
Password:<br>
<input type="password" name="password" accesskey="p" size="25"
          value="" id="password">
<br>
<input type="button" onclick="login()" value="Login" id="loginButton">
<input type="hidden" name="lang" value="" id="lan">
     <p name="errormsg" id="errormsg"></p>
</form>
</body>
</html>
```

The following figure shows the login page that the iPortal server pushes to users:



The login page shows only the mandatory elements. Other functions can be added. For example, you can add a background and set the styles of page elements.

Online Page Preparation Specification

The online page is designed to inform a user that the user has passed authentication and can use network resources normally. The file name of the login page for PCs is **login.htm**, and that for mobile STAs is **login_mobile.htm**.

- Form elements

The online page must contain a form, which is used to submit an offline request. For this reason, the form must contain a **Logout** button. The form submission method is fixed to POST. The PC online page is used as an example. Assume that the PC online page is stored in the **/portal** directory. The HTML code of the form is as follows (the HTML code of the form of the mobile STA online page is similar):

```
<form method="post" action="/portal/online.htm">
...
</form>
```

The form of the online page must contain the following page elements:

1. (Optional) Tab with the username ID: displays the information of the online user.
2. (Optional) Tab with the userip ID: displays the IP address of the online user.
3. (Optional) Tab with the usermac ID: displays the MAC address of the online user.
4. (Optional) Tab with the ssid ID: displays the SSID of the online user.
5. (Optional) Tab with the availtime ID: displays the available time during which the user can access the Internet.
6. (Mandatory) **Logout** button: allows the user to go offline and requests the display of the offline page.

When the online page is loaded, a request is sent using the GET method to retrieve user information from the server, including the user name, IP address, MAC address, and associated SSID of the online user, and available time. The URI is getonlineinfo. The onload method of the body in the HTML code must be used. The following script is used to request user information from the server (the script is only one example):

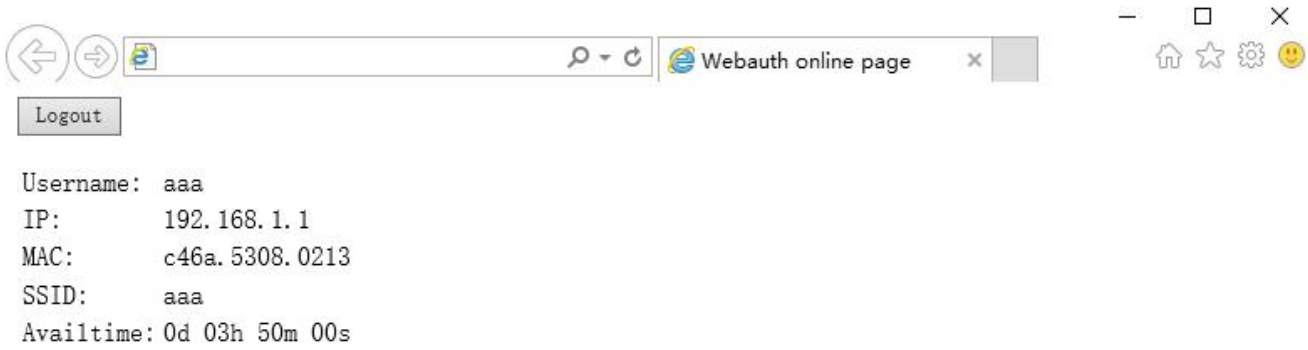
```
<script language="javascript">
//Obtain the information of the online user, including the user name, IP address, MAC address, and associated SSID of the online user, and available time.
    function requestOnlineInfo() {
        var _availTime=document.getElementById("availtime");
        var script=document.createElement("script");
        script.src="getonlineinfo"+location.search;
        _availTime.appendChild(script);
    }

    function init() {
        requestOnlineInfo();
    }
</script>
<body onload="init()">
……
</body>
```

The HTML source code of the online page is as follows:

```
<html>
<head>
<title>Web authentication online page</title>
</head>
<script language="javascript">
//Obtain the information of the online user, including the user name, IP address, MAC address, and associated SSID of the online user, and available time.
    function requestOnlineInfo() {
        var _availTime=document.getElementById("availtime");
        var script=document.createElement("script");
        script.src="getonlineinfo"+location.search;
        _availTime.appendChild(script);
```

```
    }

    function init() {
        requestOnlineInfo ();
    }
    //Script that is executed when the user clicks the Logout button. The request URI is offline.htm.
    function logout() {
        document.logoutform.action = "./offline.htm"+location.search;
        document.logoutform.submit();
        window.onbeforeunload = null;
        window.onunload = null;
    }

</script>

<body onload="init()">
<form method="post" action="/portal/offline.htm" id="logoutform">
<input type="button" onclick="logout()" value="Logout" id="logoutButton">
</form>
    <table>
    <tr><td>User name:</td><td id="username"></td></tr>
    <tr><td>IP address:</td><td id="userip"></td></tr>
    <tr><td>MAC address:</td><td id="usermac"></td></tr>
    <tr><td>Associated SSID:</td><td id="ssid"></td></tr>
    <tr><td>Available time:</td><td id="availtime"></td></tr>
    </table>
</body>
</html>
```

The following figure shows the login page that the iPortal server pushes to users:



The login page shows only the mandatory elements. Other functions can be added. For example, you can add a background and set the styles of page elements.

Offline Page Preparation Specification

The offline page is displayed when a user clicks the **Logout** button on the online page. The offline page is designed to inform the user that the user logs out successfully. If the user needs to access the Internet after logout, the user must perform authentication. The file name of the offline page for PCs is **offline.htm**, and that for mobile STAs is **offline_mobile.htm**.

The offline page has the following elements:

1. (Optional) Tab with the timeused ID: displays the time that has used by the user to access the Internet.

When the offline page is loaded, a request is sent using the GET method to retrieve the used-time information from the server. The request URI is getofflineinfo. The onload method of the body in the HTML code must be used. To obtain the used-time information, you can create a dynamic script. For example, you can create **script.src=" getofflineinfo"** to include the field information to be sent in the **src** of the script. The following script is used to request the used-time information from the server (the script is only one example):

```
<script language="javascript">
//Obtain the used time information.
    function requestOfflineInfo() {
    var _timeused =document.getElementById("timeused");
        var script=document.createElement("script");
        script.src="getofflineinfo"+location.search;
     _timeused.appendChild(script);
    }

    function init() {
         requestUserInfo();
```

```
        }
    </script>
    <body onload="init()">
    ……
    </body>
```

The HTML source code of the offline page is as follows:

```
    <html>
    <head>
    <title>Web authentication offline page</title>
    </head>
    <script language="javascript">
    //Obtain the used time information.
        function requestOfflineInfo() {
            var _timeused=document.getElementById("timeused");
            var script=document.createElement("script");
            script.src="getofflineinfo"+location.search;
            _timeused.appendChild(script);
    }

    function init() {
        requestOfflineInfo();
    }
    </script>

    <body onload="init()">
    Logout succeeded<br>
    <table>
    <tr><td>Used time:</td><td id="timeused"></td></tr>
    </table>
    </body>
    </html>
```

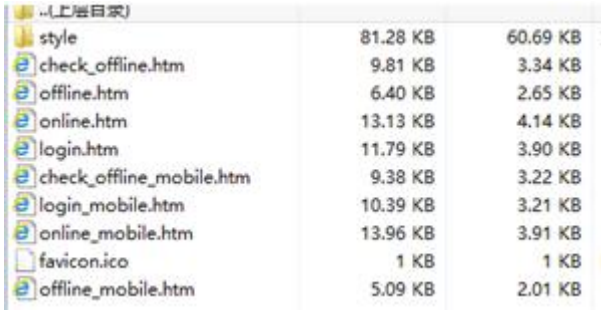
The following figure shows the offline page that the iPortal server pushes to users:

The offline page shows only the mandatory elements. Other functions can be added. For example, you can add a background and set the styles of page elements.

Page Compression Specification

After you prepare the login page, online page, and offline page in accordance with the specification described above, you need to compress the pages and related elements and upload them to the NAS. Then you can apply the page suite. The page compression specification is as follows:

1. Compress the prepared pages and related element files (such as image files and style sheet files) into a **.zip** package, for example, **portal1_page.zip**.
2. You can create directories in a page suite. For example, the **portal1_page.zip** package shown in the following figure has the **style** directory, which contains the CSS files of pages and other image files.



style	81.28 KB	60.69 KB
check_offline.htm	9.81 KB	3.34 KB
offline.htm	6.40 KB	2.65 KB
online.htm	13.13 KB	4.14 KB
login.htm	11.79 KB	3.90 KB
check_offline_mobile.htm	9.38 KB	3.22 KB
login_mobile.htm	10.39 KB	3.21 KB
online_mobile.htm	13.96 KB	3.91 KB
favicon.ico	1 KB	1 KB
offline_mobile.htm	5.09 KB	2.01 KB

After you compress the pages into a page suite, use TFTP or other tools to upload the page suite to the**/portal/zip/** directory of the flash memory on the NAS. Then configure the portal server to use the page suite (that is, associate the portal server with the page suite). For details, see the configuration manual related to Web authentication. A directory named after the page suite package is created in the/portal/ext_zip/ directory of the flash memory. For example, if the page suite package is named **portal1_page.zip**, the**/portal/ext_zip/protal1_page/** directory of the flash memory is created, and the

package is automatically decompressed in the directory. The portal server can push Web authentication pages to users based on the page suite.

Configuration Example

Customizing a Page Suite

Configuration Steps	● Customize a page suite.
	FS(config.tmplt.iportal)#page-suit fspage
Verification	● Check whether the configuration is successful.
	FS#show web-auth template Webauth Template Settings: ---------- Name: iportal Page-suit: fspage Advertising url: default Advertising mode: online-popup Type: Intral Portal Acctmlist:default Authmlist:default

15.4.22 Upgrade Compatibility

Configuration Effect

- Some configuration commands are optimized in the 11.X series software and the command formats are changed. For details, see the subsequent description.
- The 10.X series software supports smooth upgrade without function loss. However, some commands are displayed in new formats after upgrade.
- When you run the commands in earlier formats in the **no** form in the 11.X series software, a message is displayed, indicating the **no** form is not supported. You need to perform the **no** operation in new command formats.

Configuration Steps

- It is recommended that you run commands in new formats.

Verification

- Check that function loss does not occur when the 10.X series software is upgraded to the 11.X series software, and commands are displayed and stored in new formats.

- The commands in new formats have the same functions as the commands in earlier formats.

Related Commands

Configuring the Address of the Portal Server in FS First-Generation Web Authentication

Command	**http redirect homepge** *url*
Parameter Description	*url*: Indicates the address of the ePortal server in FS First-Generation Web Authentication.
Command Mode	Global configuration mode
Usage Guide	In the 11.X version, the command is converted into an eportalv1 template, and the command in template configuration mode is executed to configure and display the address of the portal server.

Configuring the Portal Server

Command	**portal-server [eportal1 | eportalv2]**
Parameter Description	**eportav1**: Indicates the information of the portal server used in FS First-Generation Web Authentication. **eportav2**: Indicates the information of the portal server used in FS Second-Generation Web Authentication.
Command Mode	Global configuration mode
Usage Guide	In the 11.X version, the command is converted into an eportalv1 or eportalv2 template, and relevant information is filled in. The main parameters of the portal server include the IP address and URL of the server. The original command will be replaced by the **ip** command and **url** command in the template.

Configuring Web Authentication Control on a Port

Command	**web-auth port-control**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	In the 11.X version, the command is converted into **web-auth enable <type>**, in which **type** specifies the type (first or second generation) of Web authentication. The default type is FS First-Generation Web Authentication.

Configuring VLAN-Based Web Authentication

Command	**web-auth allow-vlan** *list*
Parameter Description	*list*: Indicates the list of VLANs for which Web authentication is enabled.
Command Mode	Global configuration mode
Usage Guide	In the 11.X version, the command is converted into a command used to configure VLAN-based

	SCC authentication exemption.

Displaying the Configuration Information of FS First-Generation Web Authentication

Command	**show http redirect**
Parameter Description	N/A
Command Mode	Privileged mode
Usage Guide	In the 11.X version, the command is unavailable and changed to **show web-auth template**.

Displaying the Port Control Information

Command	**show web-auth port-control**
Parameter Description	N/A
Command Mode	Privileged mode
Usage Guide	In the 11.X version, the command is unavailable and changed to **show web-auth control**.

Configuration Example

Configuring FS First-Generation Web Authentication

Configuration Steps	● Check that the NAS runs on the 10.X version and is configured with the IP address of the portal server used by FS First-Generation Web Authentication.
	`FS(config)# http redirect 192.168.197.64`
	● Upgrade the NAS to 11.X.
Verification	● Run the **show running-config** command after the upgrade and check whether the new command formats are used.

	`FS#sh running-config`
	`web-auth template eportalv1`
	`  Ip 192.168.197.64`
	`!`

15.4.23 Configuring the Maximum Number of Users Sharing an Account

Configuration Effect

- Configure the maximum number of users who can use the same account to log in when account sharing is enabled during local authentication.

Notes

- This configuration takes effect for all the users that perform FS iPortal Web Authentication.

Configuration Steps

Configuring the Maximum Number of Users Sharing an Account

- Configure the maximum number of users who can share the same account in global configuration mode.

Command	web-auth account-share ip-limit xxx
Parameter Description	The value 0 indicates that the number of users who can share the same account is not limited.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Check that only a limited number of users can use the same account to go online after passing local authentication on the iPortal server, and the earliest user will be forced offline when the maximum number is exceeded.

Configuration Example

Configuring the Maximum Number of Users Sharing an Account

Configuration Steps	• Configure the maximum number of users who can share the same account.
	FS(config)#web-auth account-share ip-limit 2
Verification	• Check whether the configuration is successful.
	FS(config)#show running-config

15.4.24 Enabling iPortal Logo Replacement

Configuration Effect

- Replace the logos on all the pages displayed by the iPortal server.

Notes

- Logos are uploaded to the /data/portal/logo directory, and all logo files are named free_login_logo.jpg.

Configuration Steps

Enabling iPortal Logo Replacement in Global Configuration Mode

Command	web customized-logo enable
Parameter Description	N/A
Command Mode	Global configuration mode

Usage Guide	N/A

Verification

- Upload photos and check whether the logos on the pages displayed by the iPortal server are replaced.

Configuration Example

Enabling iPortal Logo Replacement

Configuration Steps	• Enable iPortal logo replacement. • (Optional) Enable this function only when necessary. `FS(config)#web customized-logo enable`
Verification	• Check whether the configuration is successful. `FS(config)#show running-config`

15.5 Monitoring

Clearing

Description	Command
Clears all the straight-through network resources.	**clear web-auth direct-site**
Clears all the authentication-exempted users.	**clear web-auth direct-host**
Deletes all ARP resources exempt from authentication.	**clear web-auth direct-arp**
Deletes all group information.	**clear web-auth group**

Displaying

Description	Command
Displays the basic parameters of Web authentication.	**show web-auth parameter**
Displays the Webauth template configuration.	**show web-auth template**
Displays the authentication-exempted host range.	**show web-auth direct-host [range]**
Displays the straight-through address range.	**show web-auth direct-site [range]**

Description	Command
Displays the straight-through ARP range.	**show web-auth direct-arp**
Displays the TCP interception port.	**show web-auth rdport**
Displays the Webauth configuration on a port.	**show web-auth control**
Displays the online information of all users or specified users.	**show web-auth user**{ **all** | **ip** *ip-address* / **mac** *mac-address* | **name** *name-string* | **session-id** *num* }
Displays the Webauth CGI configuration.	**show web-auth cgi**
Displays the basic global Webauth information.	**show web-auth global**
Displays the global Webauth template.	**show web-auth global authentication**
Displays the customized Webauth page suite.	**show web-auth global customized-pages**
Displays the iPortal server information.	**show web-auth global local-portal**
Displays the global Webauth template.	**show web-auth global template**
Displays the global Webauth type.	**show web-auth global webauth-type**
Displays the Webauth configuration.	**show web-auth info**
Displays the iPortal Webauth information.	**show web-auth local-portal**
Displays the Webauth mapping information.	**show web-auth ip-mapping**
Displays online and offline records about users.	**show web-auth syslog ip** *ip-address*

Debugging

System resources are occupied when debugging information is output. Disable the debugging switch immediately after use.

Description	Command
Debugs Web authentication.	**debug web-auth all**

16 Configuring Global IP-MAC Binding

16.1 Overview

Enable the global IP-MAC binding function manually to verify the input packets. If a specified IP address is bound with a MAC address, the device receives only the IP packets containing matched IP address and MAC address. The other packets are discarded.

The address bounding feature is used to verify the input packets. Note that the address binding feature takes precedence over the 802.1X authentication, port security, and access control list (ACL).

16.2 Applications

Application	Description
Global IP-MAC Binding	Only hosts with the specified IP addresses can access the network, and the hosts connected to a device can move freely.

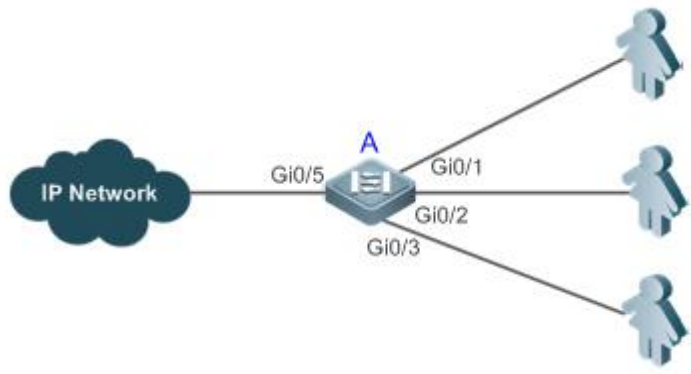
16.2.1 Global IP-MAC Binding

Scenario

The administrator assigns a fixed IP address for each host to facilitate management.

- Only hosts with the specified IP addresses can access the external network, which prevents IP address embezzlement by unauthorized hosts.
- Hosts can move freely under the same device.

Figure 16-1



Remarks	A is an access device. A user is a host configured with a static IP address. IP Network is an external IP network.

Deployment

- Manually configure the global IP-MAC binding. (Take three users as an example.)

User	MAC Address	IP Address
User 1	00d0.3232.0001	192.168.1.10

User 2	00d0.3232.0002	192.168.1.20
User 3	00d0.3232.0003	192.168.1.30

- Enable the IP-MAC binding function globally.
- Configure the uplink port (Gi0/5 port in this example) of the device as the exclude port.

16.3 Features

Basic Concepts

IPv6 Address Binding Mode

IPv6 address binding modes include Compatible, Loose, and Strict. The default mode is Strict. If IPv4-MAC binding is not configured, the IPv6 address binding mode does not take effect, and all IPv4 and IPv6 packets are allowed to pass through. If IPv4-MAC binding is configured, the IPv6 address binding mode takes effect, and the device forwards IPv4 and IPv6 packets based on the forwarding rules described in the following table:

Mode	IPv4 Packet Forwarding Rule	IPv6 Packet Forwarding Rule
Strict	Packets matching the global IPv4-MAC binding are forwarded.	Packets matching the global IPv6-MAC binding are forwarded. (The binding is generated by other access security functions, such as port security and IPv6 Source Guard.)
Loose	Packets matching the global IPv4-MAC binding are forwarded.	If IPv6+MAC address binding is configured, packets matching the IPv6-MAC binding are forwarded. (The binding is generated by other access security functions, such as port security and IPv6 Source Guard.) If IPv6-MAC binding does not exist, all IPv6 packets are forwarded.
Compatible	Packets matching the global IPv4-MAC binding are forwarded.	If the IPv6 packets contain a MAC address matching the MAC address in the IPv4-MAC binding, the IPv6 packets are forwarded. Packets matching the global IPv6-MAC binding conditions are forwarded. (The binding is generated by other access security functions, such as port security and IPv6 Source Guard.)

Exclude Port

By default, the IP-MAC binding function takes effect on all ports of the device. You can configure exclude ports so that the address binding function does not take effect on these ports. In practice, the IP-MAC bindings of the input packets on the uplink port are not fixed. Generally, the uplink port of the device is configured as the exclude port so that the packets on the uplink port are not checked for IP-MAC binding.

Overview

Feature	Description

Configuring Global IP-MAC Binding	Control forwarding of IPv4 or IPv6 packets.
Configuring the IPv6 Address Binding Mode	Change the IPv6 packet forwarding rules.
Configuring the Exclude Port	Disable the global address binding function on the specified port.

16.3.1 Configuring Global IP-MAC Binding

Working Principle

Enable the global IP-MAC binding function manually to verify the input packets. If a specified IP address is bound with a MAC address, the device receives only the IP packets containing matched IP address and MAC address. The other packets are discarded.

Related Configuration

Configuring IP-MAC Binding

Run the **address-bind** command in global configuration mode to add or delete an IPv4-MAC binding.

Enabling the IP-MAC Binding Function

Run the **address-bind install** command in global configuration mode to enable the IP-MAC binding function. By default, this function is disabled.

16.3.2 Configuring the IPv6 Address Binding Mode

Working Principle

After the global IPv4-MAC binding is configured and enabled, IPv6 packets are forwarded based on the IPv6 address binding mode. IPv6 binding modes include Compatible, Loose, and Strict.

Related Configuration

Configuring the IPv6 Address Binding Mode

By default, the IPv6 address binding mode is Strict.

Run the **address-bind ipv6-mode** command to specify an IPv6 address binding mode.

16.3.3 Configuring the Exclude Port

Working Principle

Configure an exclude port so that the address binding function does not take effect on this port.

Related Configuration

Configuring the Exclude Port

Run the **address-bind uplink** command to configure an exclude port. By default, no port is the exclude port.

16.4 Configuration

Configuration	Description and Command	
Configuring Global IP-MAC Binding	(Mandatory) It is used to configure and enable address binding.	
	address-bind	Configures a global IPv4-MAC binding.
	address-bind install	Enables the address binding function.
	address-bind binding-filter logging	Configures a logging filter of global IPv4-MAC binding.
Configuring the IPv6 Address Binding Mode	(Optional) It is used to configure the IPv6 address binding mode.	
	address-bind ipv6-mode	Configures the IPv6 address binding mode.
Configuring the Exclude Port	(Optional) It is used to disable the address binding function on a specified port.	
	address-bind uplink	Configures an exclude port.

16.4.1 Configuring Global IP-MAC Binding

Configuration Effect

- Configure a global IPv4-MAC binding.
- Enable the address binding function to control forwarding of the IPv4 or IPv6 packets.

Notes

- If you run the **address-bind install** command without IP-MAC binding configured, IP-MAC binding does not take effect and all packets are allowed to pass through.

Configuration Steps

Configuring Global IP-MAC Binding

- (Mandatory) Perform this configuration in global configuration mode.

Enabling the Address Binding Function

- (Mandatory) Perform this configuration in global configuration mode.

Configuring a Logging Filter of Global IP-MAC Binding

- (Optional) Perform this configuration in global configuration mode.

Verification

Run the **show run** or **show address-bind** command to check whether the configuration takes effect.

Related Commands

Configuring Global IP-MAC Binding

Command	**address-bind** { *ip-address* | *ipv6-address* } *mac-address*
Parameter Description	*ip-address*: Indicates the bound IPv4 address. *ipv6-address*: Indicates the bound IPv6 address. *mac-address*: Indicates the bound MAC address.
Command Mode	Global configuration mode
Configuration Usage	Run this command to configure the binding relationship between an IPv4/IPv6 address and a MAC address. This command is not supported on ACs.

Enabling the Address Binding Function

Command	**address-bind install**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	Run this command to enable the global IP-MAC binding function. This function is used to control forwarding of IPv4 or IPv6 packets. This command is not supported on ACs.

Configuring a Logging Filter of Global IP-MAC Binding

Command	**address-bind binding-filter logging** [**rate-limit** *rate*]
Parameter Description	**rate-limit** *rate*: Indicates the printing rate of logging filter of global IPv4-MAC binding.
Command Mode	Global configuration mode
Configuration Usage	By default, the rate is 10 logs per minute. When a logging filter is configured, alert logs are printed if IP packets not containing matched IP address and MAC address are detected. When a logging filter is configured, the number of non-printed logs is prompted if the actual printing rate exceeds the set rate.

Configuration Example

Configuring Global IP-MAC Binding and Enabling Address Binding

Configuration Steps	• Configure a global IPv4-MAC binding. • Enable the address binding function.
	FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# address-bind 192.168.5.1 00d0.f800.0001 FS(config)# address-bind install
Verification	Display the global IP-MAC binding on the device.
	FS#show address-bind

	Total Bind Addresses in System : 1 IP Address Binding MAC Addr --- --- 192.168.5.1 00d0.f800.0001

16.4.2 Configuring the IPv6 Address Binding Mode

Configuration Effect

- Change the IPv6 address binding mode so as to change the forwarding rules for IPv6 packets.

Configuration Steps

Configuring the IPv6 Address Binding Mode

- (Optional) Perform this configuration when you want to change the forwarding rules for IPv6 packets.

Verification

- Run the **show run** command to check whether the configuration takes effect.

Related Commands

Configuring the IPv6 Address Binding Mode

Command	**address-bind ipv6-mode** { **compatible** | **loose** | **strict** }
Parameter Description	**compatible**: Indicates the Compatible mode. **loose**: Indicates the Loose mode. **strict**: Indicates the strict mode.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuration Example

Configuring the IPv6 Address Binding Mode

Configuration Steps	• Configure a global IP-MAC binding. • Enable the address binding function. • Set the IPv6 address binding mode to Compatible.
	FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# address-bind 192.168.5.1 00d0.f800.0001 FS(config)# address-bind install FS(config)# address-bind ipv6-mode compatible

Verification	Run the **show run** command to display the configuration on the device.

16.4.3 Configuring the Exclude Port

Configuration Effect

- The address binding function is disabled on the exclude port, and all IP packets can be forwarded.

Notes

- The configuration can be performed only on a switching port or an L2 aggregate port.

Configuration Steps

Configuring the Exclude Port

- (Optional) Perform this configuration in global configuration mode when you want to disable the address binding function on a specified port.

Verification

Run the **show run** or **show address-bind uplink** command to check whether the configuration takes effect.

Related Commands

Configuring the Exclude Port

Command Syntax	**address-bind uplink** *interface-id*
Parameter Description	*interface-id*: Indicates the ID of a switching port or an L2 aggregate port.
Command Mode	Global configuration mode
Configuration Usage	This command is not supported on ACs.

Configuration Example

Configuring the Exclude Port

Configuration Steps	• Create a global IPv4-MAC binding. • Enable the address binding function. • Configure an exclude port.
	FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# address-bind 192.168.5.1 00d0.f800.0001 FS(config)# address-bind install FS(config)# address-bind uplink GigabitEthernet 0/1

Verification	Display the global IP-MAC binding on the device.
	FS#show address-bind Total Bind Addresses in System : 1 IP Address Binding MAC Addr --- --- 192.168.5.1 00d0.f800.0001 FS#show address-bind uplink Port State --- --- Gi0/1 Enabled Default Disabled

16.5 Monitoring

Displaying

Description	Command
Displays the IP-MAC binding on the device.	**show address-bind**
Displays the exclude port.	**show address-bind uplink**

17 Configuring IPoE

17.1 Overview

IPoE authentication implements authentication and charging for a client based on the MAC address of the client. No account or password is required for Internet access of the client.

IPoE supports authentication, authorization, accounting (AAA).

Authentication: Authenticates whether the client has access permission to prevent illegal clients.

Authentication: Authorizes clients with available services and controls the access permission of legal clients.

Accounting: Records usage of network resources of clients to provide basis for charging.

IPoE can be deployed in the network that controls client access, so as to implement services such as client authentication and authorization.

Protocols and Standards

- RFC2131: Dynamic Host Configuration Protocol
- RFC2132: DHCP Options and BOOTP Vendor Extensions
- RFC3046: DHCP Relay Agent Information Option

17.2 Applications

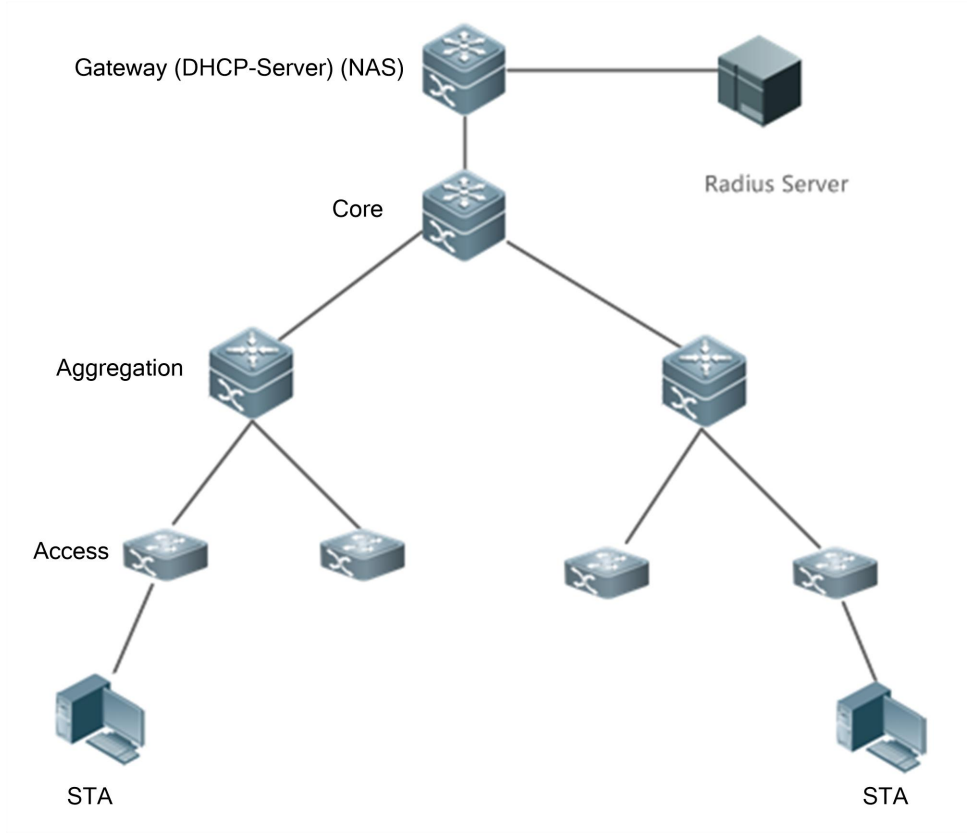
Application	Description
Applying IPoE Client Authentication	The DHCP client accesses the gateway in IPoE mode via the layer-3 network.

17.2.1 Applying IPoE Client Authentication

Scenario

- The DHCP client accesses the access device via the layer-2 network and accesses the gateway in IPoE mode via the layer-3 network.
- The access device, as a DHCP relay, applies to the gateway for an IP address.
- A RADIUS server is adopted as the server for authentication, authorization, and charging.

Figure 177- 1 DHCP Packet Triggering IPoE Access



Deployment

- Enable the IPoE function on the gateway.
- Enable the PC client to obtain the IP address via DHCP.
- Enable the PC client to access the Internet via web authentication.

17.3 Features

Basic Concepts

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a remote authentication protocol defined by RFC2865 and has a wide support range. Remote deployment and authentication of servers can be implemented by using this protocol. IPoE is usually deployed remotely on the server and the IPoE authentication information is transmitted via RADIUS between the device and the server.

Timeout

The switch needs to communicate with the client and server during authentication. If the client or server does not respond in the specified period of time in the protocol, it is considered that the authentication times out, which causes an authentication failure. During actual deployment, IPoE and RADIUS both have their own timeout period. Therefore, the timeout period of IPoE must be longer than that of RADIUS when they are both used.

Authorization

The client will be bounded with certain services (such as IP address and QoS) after passing authentication.

Charging

It implements client network audit, such as time of accessing the network and generated traffic, which facilitates network management and maintenance.

Some RADIUS servers, such as FS SAM+ and SMP servers, determine the online/offline status of clients based on charging packets. Therefore, the charging function is mandatory when these servers are used as RADIUS servers.

Overview

Feature	Description
IPoE Cient Authentication	Provides secure access for clients. Only clients passing authentication have access to the network.

17.3.1 IPoE Client Authentication

Working Principle

IPoE authentication implements authentication and charging for a client based on the MAC address of the client. No account or password is required for Internet access of the client.

IPoE authentication provides the following function:

IPoE Client Authentication

IPoE authentication implements authentication and charging for a client based on the MAC address of the client. No account or password is required for Internet access of the client.

Related Configuration

Enabling IPoE Function

- The IPoE function of the device is disabled by default.
- Run the **ipoe-auth enable** command to enable or disable the IPoE function.
- IPoE can work only after it is enabled on the device.

17.4 Configuration

Configuration	Description and Command	
Enabling IPoE Function	(Mandatory) It is used to set up the IPoE service.	
	ipoe-auth enable	Enables the IPoE function on the device and specifies the client access mode.
	Optional	

	ipoe-auth dhcp user-limit	Configures the maximum number of allowed IPoE sessions triggered by DHCP packets.
	ipoe-auth quiet-period	Configures the silent time of clients authenticated via IPoE.
	ipoe-auth server-timeout	Configures authentication timeout period.

17.4.1 Enabling IPoE Function

Configuration Effect

Enable the IPoE function to provide clients with secure access. Only clients passing authentication have access to the network.

Configuration Steps

Enabling IPoE Function

- Mandatory.
- The IPoE function can be enabled if no special requirement is raised.

Configuring Maximum Number of Allowed IPoE Sessions Triggered by DHCP Packets

- Optional.
- The maximum number of IPoE sessions is not limited by default, and can be configured as required.

Configuring Silent Time of Clients Authenticated via IPoE

- Optional.
- The silent time function of clients is disabled by default. The waiting interval after an authentication failure can be configured as required.

Configuring Authentication Timeout Period

- Optional.
- The default timeout period is 25 seconds. If the timeout period of the RADIUS server is longer than 25 seconds, a larger value can be configured.

Verification

- Run the **show run** command to display the IPoE configuration status.

Related Commands

Enabling IPoE Function

Command	**ipoe-auth enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	The IPoE function can be enabled if no special requirement is raised.

Configuring Maximum Number of Allowed IPoE Sessions Triggered by DHCP Packets

Command	**ipoe-auth user-limit** *number*
Parameter Description	*Number*: Indicates the maximum number of allowed IPoE sessions triggered by DHCP packets. The value ranges from 1 to 1,000,000. No input is equivalent to the value 0 by default, indicating no limit.
Command Mode	Global configuration mode
Usage Guide	When the number of IPv4 IPoE authentication sessions triggered by DHCPv4 packets reaches the maximum value, subsequent DHCPv4 packets cannot trigger creation of IPv4 IPoE authentication sessions.

Configuring Silent Time of Clients Authenticated via IPoE

Command	**ipoe-auth quiet-period** *time*
Parameter Description	*time*: Indicates the silent time. The value ranges from 0 to 65,535 seconds. No input is equivalent to the value 10 by default.
Command Mode	Global configuration mode
Usage Guide	This command is used to set the waiting interval after an authentication failure. During the silent time, the device directly discards packets from the client that fails authentication, to avoid the device from continuously sending packets to the server, thereby preventing impact on the device performance.

Configuring Authentication Timeout Period

Command	**ipoe-auth server-timeout** *time*
Parameter Description	*time*: Indicates the timeout period. The value ranges from 1 to 65,535 seconds. No input is equivalent to the value 30 by default.
Command Mode	Global configuration mode
Usage Guide	This command is used to ensure that the IPoE timeout period is longer than that of the RADIUS server.

Configuration Example

Enabling IPoE Function

Configuration Steps	● Enable the IPoE function on the gateway.
	FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# ipoe-auth enable FS(config)# exit
Verification	● Check whether the IPoE function is enabled. FS# show run | include ipoe-auth ipoe-auth enable

17.5 Monitoring

Clearing

Description	Command
Clears IPoE authenticated clients by forcing them to go offline.	**clear ipoe-auth user**

Displaying

Description	Command
Displays entries of IPoE authenticated clients.	**show ipoe-auth summary**
Displays details about IPoE authenticated clients.	**show ipoe-auth user**

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs the IPoE event.	**debug ipoe event**

18 Configuring IP Group

18.1 Overview

The IP address group feature uses IP address lists to implement IP address matching. Currently, the following IP address lists are supported:

- IP address range list
- IP network segment list
- Routing address database list

18.2 Applications

The IP address group feature is used together with other modules. It is not used independently. For example, the accounting module uses the IP address group feature to exempt specified IP addresses from traffic accounting.

18.3 Features

Basic Concepts

↘ ip-group

An IP address group contains an IP network segment and an IP address range used to match IP addresses to the IP address group.

Overview

Feature	Description
ip-group	Matches IP addresses to an IP address group.

18.3.1 ip-group

An IP address group contains an IP network segment and an IP address range used to match IP addresses to the IP address group.

Working Principle

The IP address group feature implements IP address matching by taking the following steps:

1. Create an IP address group.
2. Configure an IP network segment or an IP address range for the IP address group.
3. Match IP addresses to the IP address group.

Related Configuration

↘ Configuring the IP Address Group Feature

The IP address group feature includes the following configuration items:

- (Optional) Configuring an IP address group

Run the **ip-group** *id* command in global configuration mode to create or configure an IP address group. Run the **no ip-group** *id* command to delete an IP address group. *id* indicates the IP address group index.

- (Optional) Configuring IP address group description

Run the **descrption** *name* command in IP address group configuration mode to configure IP address group description. Run the **no descrption** command to delete IP address group description.

- (Optional) Configuring an IP address range

Run the **ip-range** *start [end]* command in IP address group configuration mode to configure an IP address range. Run the **no ip-range** *start [end]* command to delete an IP address range.

- (Optional) Configuring an IP network segment

Run the **ip-subnet** *subnet { mask | mask_len }* command in IP address group configuration mode to configure an IP network segment. Run the **no ip-subnet** *subnet { mask | mask_len }* command to delete an IP network segment.

- (Optional) Configuring a routing address database

Run the **route-db** *name* command in IP address group configuration mode to configure a routing address database list. Run the **no route-db** *name* command to delete a routing address database list.

18.4 Configuration

Configuration	Description and Command	
Configuring the IP Address Group Feature	⚠ Mandatory. It is used to configure an IP address list for an IP address group.	
	ip-group *id*	Configure an IP address group.
	ip-range *start [end]*	Configure an IP address range.
	ip-subnet *subnet { mask | mask_len }*	Configure an IP network segment.
	route-db *name*	Configures a routing address database list.

18.4.1 Configuring the IP Address Group Feature

Configuration Effect

Implement IP address matching.

Notes

N/A

Configuration Steps

Configuring an IP Address Group

- Optional.

Command	**ip-group** *id*
Parameter	The ID ranges from 1 to 1,000.

Description	
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	To delete an IP address group, run the **no ip-group** *id* command.

Configuring IP Address Group Description

- Optional.

Command	**Descrption** *name*
Parameter Description	*name*: descriptive string, which consists of up to 32 characters and cannot contain spaces
Defaults	By default, no IP address group description is configured.
Command Mode	IP address group configuration mode
Usage Guide	To delete the descriptive string, run the **no descrption** command in IP address group configuration mode.

Configuring an IP Address Range

- Optional.

Command	**ip-range** *start [end]*
Parameter Description	*start*: Indicates the start IP address of the network segment. *end*: Indicates the end IP address of the network segment. By default, the values of *start* and *end* are the same.
Defaults	By default, no IP address range is configured.
Command Mode	IP address group configuration mode
Usage Guide	To delete an IP address range, run the **no ip-range** *start [end]* command in IP address group configuration mode.

Configuring an IP Network Segment

- Optional.

Command	**ip-subnet** *subnet { mask | mask_len }*
Parameter Description	*subnet*: Indicates the start address of the IP network segment. *mask*: Indicates the mask. *mask_len*: Indicates the mask length.
Defaults	By default, no IP network segment is configured.
Command Mode	IP address group configuration mode
Usage Guide	To delete an IP network segment, run the **no ip-subnet** *subnet mask_len* command in IP address group configuration mode.

Configuring a Routing Address Database List

- Optional.

Command	**route-db** *name*
Parameter Description	*name*: Indicates the name of the routing address database list.
Defaults	By default, no routing address database is configured.
Command Mode	IP address group configuration mode
Usage Guide	To delete a routing address database list, run the **no route-db** *name* command in IP address group configuration mode.

Verification

Run the **show** command to display:

- IP address group configurations
- Matching results by IP address group ID and IP address

Configuration Example

Configuring an IP Address Group and an IP Network Segment

Scenario	N/A
Configuration Steps	● Configure an IP address group. FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# ip-group 1 FS(config-ip-group)# descrption test FS(config-ip-group)#ip-range 1.1.1.5 1.1.1.10 FS(config-ip-group)#ip-subnet 1.1.10.0 24 FS(config-ip-group)#route-db cmc

18.5 Monitoring

Displaying

Description	Command
Displays IP address group configurations.	**show ip-group** [*id*]
Displays IP address group statistics.	**show ip-group statistics**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command

Enable IP address group ctrl debugging.	**debug ip-group ctrl**
Disable IP address group ctrl debugging.	**no debug ip-group ctrl**
Enable IP address group db-ctrl debugging.	**debug ip-group db-ctrl**
Disable IP address group db-ctrl debugging.	**no debug ip-group db-ctrl**

19 Configuring Link SAM

19.1 Overview

Link SAM is the module on FS gateway devices used to communicate with the SAM+. It receives authenticated users' information from the SAM+ and sends these users' traffic statistics to the authentication and accounting server. The gateway and authentication and accounting server must be deployed together when the SAM+ performs authentication and accounting for intranet users. With a switch as an ingress NAS or a gateway as an egress NAS, redirection authentication is applied to unauthenticated intranet users. After the users pass the authentication, the authentication and accounting server sends authenticated users' information to the gateway, and the gateway notifies the authentication and accounting server of online users' traffic usage.

- Because the SAM+ has several message formats used for egress device communication, the Link SAM feature varies with different devices. The Link SAM in this document refers to the module of the gateway that correlates with an SAM+ or a remote database. Currently, authentication is supported on EG series, ACE series and MSC gateways, and not on NBR series gateways.
- EG series and ACE series apply different protocols to their correlation with the SAM+. They are distinguished via configuration. MSC cards obtain information from the N18000 switches via databases rather than from its correlation with the SAM+.
- For gateways supporting IPFIX accounting, LINK-SAM must be run to guarantee the proper operation of IPFIX modules. IPFIX accounting is supported on EG2000XE/UE/ACE series/MSC cards.

19.2 Applications

Application	Description
MSC-SAM+ Correlation	Link SAM, integrated with the SAM+ system, is configured to implement authentication, accounting, and extranet access check.

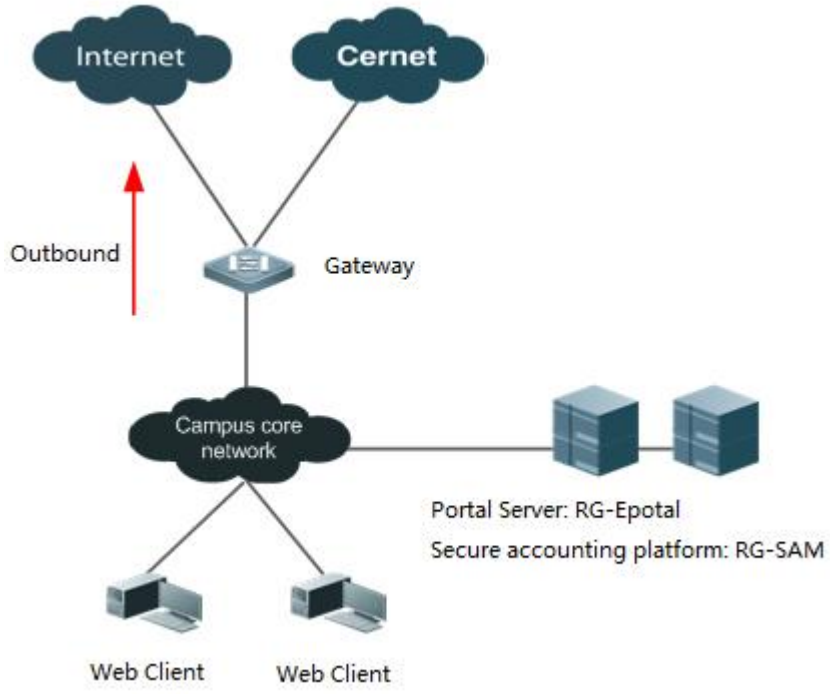
19.2.1 Gateway-SAM+ Correlation

Scenario

The gateway is correlated with the SAM+ to implement authentication, accounting, and extranet access check. See Figure 19-1

- The gateway redirects the traffic of unauthenticated users to the Eportal server for Web authentication.
- The Eportal server sends the information of users requiring Web authentication to the SAM+ authentication and accounting platform.
- If a user passes authentication, the user can go online. The SAM+ then sends the user information to the gateway.
- The gateway periodically notifies the SAM+ (gateways supporting IPFIX accounting) of the user's traffic usage.

Figure 19-1



Deployment

- Enable the Link SAM module on the gateway to communicate with the FS-SAM.
- Enable the Web authentication module on the gateway to redirect the URLs of unauthenticated users to the FS-Eportal and implement extranet access restriction.
- Enable the IPFIX module on the gateway to collect statistics on the traffic usage of online users.

19.3 Features

Basic Concepts

Flow

A flow or streaming session consists of packets sent during a period and with the same quintuple (source IP address, source port, destination IP address, destination port, and VPN routing and forwarding [VRF]).

Authenticated User

An authenticated user is an intranet user who has passed FS Web authentication or 802.1X authentication before accessing the extranet. The FS SAM+ authentication and accounting system assigns identity information and accounting methods to authenticated users. Currently, the SAM+ supports a one-to-one relationship between IP addresses and users.

Link SAM with SAM+ System Integration

Link SAM with SAM+ system integration enables sharing of authenticated user information between routing of user access requests and the SAM+ system. When an authenticated user goes online, the SAM+ sends

information about the user's IP address and user group to the Layer-2/3 classification and identification module of the gateway.

User Information

When an authenticated user goes online, the SAM+ sends the user's information to the Layer-2/3 classification and identification module of the gateway if Link SAM with SAM+ system integration is enabled. The sent information includes the user's IP address and user group.

Overview

Feature	Description
Communication with the Authentication and Accounting Server	Sends traffic usage statistics and SAM+ synchronization information.
Link SAM Protocol	Configures the protocol version of the Link SAM module. By default, the v2 (3.90) protocol version is used.
Link SAM with SAM+ System Integration Timeout	Sets the Link SAM with SAM+ system integration timeout time. The value ranges from 2 to 150,000, in minutes. The default timeout time is 2 minutes for traffic accounting and 20 minutes for non-traffic accounting.
Packet Rate Limiting	Controls traffic flows effectively.

19.3.1 Communication with the Authentication and Accounting Server

The authentication and accounting gateway communicates with the SAM+, or other authentication and accounting server through the Link SAM module, which sends the information received from the authentication and accounting server to the IPFIX module and other internal functional modules. The Link SAM module provides an interface for the internal functional modules to communicate with the authentication and accounting server.

Working Principle

The Link SAM module adopts the TCP socket and listens to local Port 2009 on ACE series/Port 2012 on EG series by default to receive SAM+ connection requests. The SAM+ sets up a connection to the gateway through Port 2009 and sends online user information. If multiple SAM+s exist, each SAM+ initiates a connection to the Link SAM module.

The SAM+ enables Port 4739 for receiving Link SAM connection requests. After the Link SAM module is connected to the SAM+, the gateway's IPFIX module collects statistics on the traffic usage of online users and the Link SAM module sends the statistics to the SAM+. If multiple SAM+s exist, the Link SAM module needs to initiate connections to all SAM+s.

Setting the Name of the Authentication and Accounting Server

By default, no authentication and accounting server is specified for the Link SAM module. Because multiple servers may exist, you can run the **link-sam auth-server ip** *ip-address* [**port** *port-number*] command to specify the authentication and accounting server.

The authentication and accounting server does not need to be specified if the gateway does not notify the server of traffic usage.

19.3.2 Link SAM Protocol

For ACE series, Link SAM with SAM+ system integration is developed based on the SAM+ 3.90 version but also compatible with earlier versions. By default, versions later than 3.90 are supported. For EG series, versions earlier than SAM+ 3.90 are supported, but versions earlier than 3.90 are recommended to use.

Working Principle

Link SAM with SAM+ system integration is compatible with versions earlier than the SAM+ 3.90 to allow the Link SAM module to communicate with the SAM+.

19.3.3 Link SAM with SAM+ System Integration Timeout

If the Link SAM module receives no messages from the SAM+ for a period, the communication between them has an error and the Link SAM module closes the SAM+ connection. Such a period is called the Link SAM with SAM+ system integration timeout time. Link SAM with SAM+ system integration is either in the online or offline state. If the communication between all SAM+s and the Link SAM module times out, the SAM+s are offline; otherwise, they are online.

Working Principle

When Link SAM with SAM+ system integration times out, the Link SAM module cannot receive information synchronized from the SAM+ server.

19.3.4 Packet Rate Limiting

The processing of online user traffic usage statistics by the authentication and accounting server requires high performance, which may make some packets go unprocessed. To address this problem, you can rate-limit the packets that the Link SAM module sends to the authentication and accounting server.

Working Principle

The Link SAM module has a message cache queue, which temporarily stores traffic usage statistics to be sent. The packet sending rate can be limited by controlling the rate of retrieving packets from the cache queue.

19.4 Configuration

Configuration	Description and Command	
Configuring Basic Link SAM Functions	(Mandatory) It is used to enable the Link SAM feature.	
	link-sam enable	Enables the Link SAM feature.

	link-sam auth-server ip *ip-address* **port** *port-number*	Specifies the authentication and accounting server.
	(Optional) It is used to configure the Link SAM local port.	
	link-sam flowrate *rate*	Configures Link SAM rate limiting.
	link-sam port *port-number* [**ace**]	Configure the local listening port for the Link SAM module.

19.4.1 Configuring Basic Link SAM Functions

Configuration Effect

- Enable the Link SAM module to receive and send messages from/to the authentication and accounting server.
- To obtain authenticated users' information, EG series and ACE series depend on the Link-SAM with SAM+ system while MSC cards on connection with databases.

Notes

- The listening port and connection port on the authentication and accounting server must be configured correctly.
- The IPFIX feature must be enabled on the gateway in order to collect statistics on the traffic usage of online users and send the statistics to the related device.

Configuration Steps

Enabling the Link SAM Feature

- Mandatory.

Command	**link-sam enable**
Parameter Description	*address*: IP address of the remote database
Defaults	By default, the Link SAM feature is disabled.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure Link SAM with SAM+ system integration or connect the Link SAM module to a remote database. By default, Link SAM with SAM+ system integration is configured. Configure the IP address of the database in MSC Card mode.

Specifying the Authentication and Accounting Server

- Mandatory.

Command	**link-sam auth-server ip** *ip-address* [**port** *port-number*]
Parameter Description	*ip-address*: IP address of the authentication and accounting server *port-number*: port number of the authentication and accounting server
Defaults	By default, no authentication and accounting server is specified.

Command Mode	Global configuration mode
Usage Guide	Run this command to specify the authentication and accounting server when multiple servers exist. The Link SAM module sends traffic usage statistics to the authentication and accounting server through TCP. The authentication and accounting server is at the server end, and the Link SAM module is at the client end.

Configuring Link SAM Rate Limiting

- Optional.

Command	**link-sam flowrate** *rate*
Parameter Description	*rate*: rate at which the Link SAM module is controlled to send packets
Defaults	The default value is 22.
Command Mode	Global configuration mode
Usage Guide	Run this command to control the rate at which the Link SAM module sends packets.

Configuring the Local Listening Port for the Link SAM Module

- Optional.

Command	**link-sam port** *port-number* **[ace]**
Parameter Description	*port-number*: number of the local listening port for the Link SAM module
Defaults	The default value is 2009.
Command Mode	Global configuration mode
Usage Guide	Run this command to specify the local listening port for the Link SAM module. The authentication and accounting server sends online user information to the Link SAM module through TCP. The Link SAM module is at the server send, and the authentication and accounting server is at the client end.

Verification

Connect the MSC to the SAM+ for synchronized communication.

- Check whether the MSC can receive user information packets synchronized from the SAM+.

Configuration Example

The following configuration is based on the Link-SAM module of the ACE series.

Enabling the Link SAM Feature

Scenario	The Link SAM module needs to be connected to the SAM+ accounting device.
Configuration Steps	• Enable the Link SAM feature in global configuration mode. FS# configure terminal

	Enter configuration commands, one per line. End with CNTL/Z. FS(config)# link-sam enable ● Specify the authentication and accounting server. FS(config)# link-sam auth-server ip 192.168.5.42 ● Configure rate limiting. FS(config)# link-sam flowrate 50
Verification	Configure Link SAM with SAM+ system integration. ● Run the **show link-sam statistics ace** command to display statistics on Link SAM with SAM+ system integration. FS#show link-sam statistics ace >Link-sam run state: enable[sam_state: up] >Link-sam connect port: 2009 >Link-sam connect timeout minutes: 2 >Current SAM connections: 1 >Count of SAM connections: 2 >Count of SAM disconnections: 1 ---------- link-sam flowrate 30 link-sam auth-server ip 192.168.5.42 ---------- SAM's ip: 192.168.5.42 Received packets: 13159 Received user online messages: 228 Received user offline messages: 202 Received user synchronization messages: 9580 Received user ip update messages: 0 Received exception messages: 0 Received invalid segments: 0

Scenario	The Link SAM module needs to be connected to a database.
Configuration Steps	● Enable the Link SAM feature in global configuration mode. FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z.

	FS(config)# link-sam enable db-ip 192.168.1.1
Verification	Check the database connection status of the Link SAM module. ● Run the **show link-sam statistics** command to display the database connection status of the Link SAM module. FS(config)#show link-sam statistics >Link-db run state: enable >Link-db server: 192.168.25.241 >Link-db state: down >Link-db cnt: 0. >Link-db syn event: 3. >Link-db update failed event: 0 >Link-db online event: 0. >Link-db offline event: 0. >Link-db error event: 0.

Common Errors

- The port configuration of the authentication and accounting server is incorrect.

19.5 Monitoring

Clearing

Description	Command
Clears statistics on Link SAM with SAM+ system integration.	**clear link-sam statistics [ace]**

Displaying

Description	Command
Displays statistics on Link SAM with SAM+ system integration.	**show link-sam statistics [ace]**

20 Configuring FLOW ACCOUNT

20.1 Overview

Internet Protocol Flow Information Export (IPFIX) is a method for collecting statistics on traffic flows on a per-user basis.

IPFIX periodically sends users' traffic flow accounting information to an accounting server based on the users' accounting service network, and synchronizes the users' online status.

20.2 Applications

N/A

20.3 Features

Basic Concepts

➘ Flow

A flow or streaming session consists of packets sent during a period and with the same quintuple (source IP address, source port, destination IP address, destination port, and VPN routing and forwarding [VRF]).

Overview

Feature	Description
IPFIX Switch	Enables and disables the IPFIX module.
IPFIX Policy	Configures IPFIX policies.
IPFIX Policy Priority	Adjusts the priorities of IPFIX policies.
IPFIX Threshold Switch	Enables and disables IPFIX traffic threshold notification.
IPFIX Detection Period Switch	Enables and disables IPFIX periodic no-traffic detection.
IPFIX Detection Period	Notifies the SAM of users' no-traffic information periodically.
IPFIX Whitelist	Exempts URLs from accounting.

20.3.1 IPFIX Switch

The IPFIX switch is used to enable and disable the IPFIX module.

Working Principle

When the IPFIX switch is turned on, the IPFIX module collects statistics on users' traffic flows.

When the IPFIX switch is turned off, the IPFIX module does not collect statistics on users' traffic flows.

20.3.2 IPFIX Policy

IPFIX policies are used to classify users' traffic flows.

Working Principle

Traffic flows are matched to IPFIX policies and then are classified.

By default, all traffic flows are classified into campus traffic. After IPFIX policies are configured, traffic flows are matched to those policies and classified into different types.

20.3.3 IPFIX Policy Priority

Traffic flows are matched according to IPFIX policy priorities, which can be adjusted to modify traffic matching and classification.

Working Principle

IPFIX policies with higher priorities are preferentially used for matching.

20.3.4 IPFIX Traffic Threshold Switch

The IPFIX traffic threshold switch is used to enable and disable traffic threshold notification.

Working Principle

The IPFIX module compares the traffic available for use to a threshold. If the available traffic is smaller or equal to the threshold, the IPFIX module notifies the SAM. If the available traffic is greater than the threshold, the IPFIX module does not notify the SAM.

20.3.5 IPFIX Detection Period Switch

The IPFIX detection period switch is used to enable and disable IPFIX periodic no-traffic detection.

Working Principle

After no-traffic detection is enabled, the IPFIX module periodically detects users' traffic usage. If traffic usage is zero, the IPFIX module notifies the SAM. If traffic usage is not zero, the IPFIX module does not notify the SAM.

20.3.6 IPFIX Detection Period

The IPFIX detection period is the period when the IPFIX module performs no-traffic detection and notifies the SAM of detection results.

Working Principle

After the detection period is configured, the IPFIX module periodically detects users' traffic usage. If traffic usage is zero, the IPFIX module notifies the SAM.

20.3.7 IPFIX Whitelist

The IPFIX whitelist feature is used to exempt URLs from accounting.

Working Principle

The traffic of access to URLs in the whitelist is exempt from accounting.

20.4 Configuration

Configuration	Description and Command	
Configuring IPFIX	(Mandatory) It is used to configure IPFIX.	
	ipfix enable	Enables the IPFIX module.
	ipfix policy *num* **{acl** *acl-num* **| src-group** *group-id* **dst-group** *group-id* **} action {home | foreign | campus | unicom | telecom | cmcc | cernet | cernet2 | direct-flow} [interface** *id* **]**	Configures IPFIX policies.
	(Optional) It is used to configure IPFIX traffic detection and notification.	
	ipfix refresh enable	Enables no-traffic detection.
	ipfix refresh-time *time*	Sets the no-traffic detection period.
	Ipfix direct-url *url*	Configures a whitelist.

20.4.1 Configuring IPFIX

Configuration Effect

Match and classified traffic flows according to IPFIX policies, and collect statistics on traffic flows on a per-user basis. Enable the IPFIX module to periodically detect users' traffic usage (the default period is 10 minutes). If traffic usage is zero, the IPFIX module sends an abnormal go-offline message to the SAM.

Configuration Steps

Enabling the IPFIX Module

- Mandatory.

Command	**Ipfix enable**
Parameter Description	N/A
Defaults	By default, the IPFIX module is disabled.
Command Mode	Global configuration mode
Usage Guide	To disable the IPFIX module, run the **no ipfix enable** command.

Configuring IPFIX Policies

- Mandatory.

Command	**ipfix policy** *num* **{acl** *acl-num***| src-group** *group-id* **dst-group** *group-id* **}action {home | foreign | campus| unicom | telecom | cmcc | cernet | cernet2 | direct-flow} [interface** *id* **]**
Parameter Description	*num*: Indicates the policy name. The value ranges from 1 to 100.
	acl-num: Indicates the ID of the bound access control list (ACL) module. *group-id*: Indicates the ip-group ID. The value ranges from 0 to 1,000. The value 0 indicates

	matching any traffic types. *id*: Indicates the interface ID (the interface must be a non-LAN interface). **home**: Indicates domestic traffic. **foreign**: Indicates international traffic. **campus**: Indicates campus traffic. **unicom**: Indicates China Unicom. **telecom**: Indicates China Telecom. **cmcc**: Indicates China Mobile. **cernet**: Indicates the China Education and Research Network. **cernet2**: Indicates the second-generation China Education and Research Network. direct-flow: Indicates the traffic exempt from accounting.
Defaults	On gateways, the default IPFIX policy is campus traffic matching.
Command Mode	Global configuration mode
Usage Guide	To delete IPFIX policies, run the **no ipfix policy** *num* command in global configuration mode. After IPFIX policies are configured, users' traffic flows are matched to those policies and classified into different types for statistics.

Enabling IPFIX No-traffic Detection

- Optional.

Command	**ipfix refresh enable**
Parameter Description	N/A
Defaults	By default, IPFIX no-traffic detection is disabled.
Command Mode	Global configuration mode
Usage Guide	To disable IPFIX no-traffic detection, run the **no ipfix refresh enable** command.

Setting the No-traffic Detection Period

- Optional.

Command	**ipfix refresh-time** *time*
Parameter Description	*time*: Indicates the no-traffic detection period. The value ranges from 600 to 3,600, in seconds.
Defaults	The default detection period is 600s.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring a Whitelist

- Optional.

Command	**ipfix direct-url** *url*
Parameter Description	*url*: Indicates URL strings.

Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	You can configure up to 1,000 URL resolution records.

Displaying the IPFIX Module Configurations

Command	**show ipfix configure**
Parameter Description	N/A
Defaults	N/A
Command Mode	Privileged mode, global configuration mode, or interface configuration mode
Usage Guide	To display the IPFIX module configurations, run the **show ipfix configure** command.

Displaying the IPFIX Policy Status

Command	**show ipfix policy**
Parameter Description	N/A
Defaults	N/A
Command Mode	Privileged mode, global configuration mode, or interface configuration mode
Usage Guide	To display the IPFIX policy status, run the **show ipfix policy** command.

Displaying the IPFIX Node Status

Command	**show ipfix online [user** *user-name* **| ip** *ip-addr*| **count]**
Parameter Description	*user-name*: Indicates the user ID. *ip-addr*: Indicates the user's IP address.
Defaults	N/A
Command Mode	Privileged mode, global configuration mode, or interface configuration mode
Usage Guide	To display the IPFIX node status, run the **show ipfix online [user** *user-name* **| ip** *ip-addr*| **count]** command.

Verification

Collect statistics on traffic usage on a per-user basis.

- Check whether traffic flows are matched by type.
- Check whether the IPFIX module configurations take effect.
- Display online user information.
- Display the resolution records of the whitelist.

Configuration Example

Enabling the IPFIX Module and Configuring IPFIX Policies

Scenario	A university's accounting system consists of the SAM and an authentication and accounting gateway.
Configuration Steps	● Enable IPFIX in global configuration mode. FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# ipfix enable ● Configure ACLs. FS(config)# ip access-list standard 1 FS(config-std-nacl)#permit any FS(config-if-dialer 1)# end FS(config)# ip access-list standard 2 FS(config-std-nacl)#permit 192.168.1.0 0.0.0.255 FS(config-if-dialer 1)# end ● Configure IPFIX policies. FS(config)# ipfix policy 1 acl 1 action home interface GigabitEthernet 0/3 FS(config)# ipfix policy 2 acl 2 action foreign interface GigabitEthernet 0/3 ● Enable IPFIX no-traffic detection. FS(config)#ipfix refresh enable
Verification	Display IPFIX information. ● Run the **show ipfix configure** command to display the IPFIX module configurations. FS(config)#show ipfix configure ipfix configure: ipfix state: enable ipfix threshold state: disable ipfix refresh state: enable ipfix refresh-time: 600s ipfix policy 1 acl 1 action home interface GigabitEthernet 0/3 ipfix policy 2 acl 2 action foreign interface GigabitEthernet 0/3 ipfix policy 3 src-group 1 dst-group 2 action home ● Run the **show ipfix policy** command to display the IPFIX policy status. FS(config)#show ipfix policy Policy Acl Src-grp Dst-grp Priority Interface Action Disable State ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- 1 1 0 0 0 Gi0/3 home n active 2 1 0 0 1 Gi0/3 foreign n active 3 0 1 2 2 Global home n active ● Run the **show ipfix online** command to display online user information. FS(config)#show ipfix online

```
User-id      Ip                    Samtime(M) Samflow(M) Time(M)      Flow(M)      Campus(M)
Home(M)                Foreign(M)
----------  ----------------  ----------  ----------  ----------  ----------  ------------------  ------------------
------------------
yangzhenyu 192.168.231.27     35364         104857600    433            0               0/0
0/0                    0/0
wuyunzhi     172.18.124.27      345600        8530          11             0               0/0
0/0                    0/0
yinwei        172.18.124.19      345600        8259          161            0               0/0
0/0                    0/0
yangjm        192.168.225.52     345600        10152         433            0               0/0
0/0                    0/0
hongyingming 172.18.124.54      345600        7910          433            0               0/0
0/0                    0/0
caibiyun      192.168.225.74     345600        10064         433            0               0/0
0/0                    0/0
chenweiyao 172.18.124.45      345600        8793          433            0               0/0
0/0                    0/0
```

- Run the **show ipfix direct-url** command to display the IPFIX whitelist.

```
FS#show ipfixdirect-url
URL[0]    www.baidu.com
RESOLVE-IP:        115.239.210.27 115.239.211.112
URL[1]    www.fs.net
RESOLVE-IP:        192.168.5.102
```

Common Errors

- Configurations do not take effect because the IPFIX module is not enabled.
- IPFIX policies do not take effect because no ACLs are configured.

20.5 Monitoring

Displaying

Description	Command
Displays the IPFIX module configurations.	**show ipfix configure**
Displays the IPFIX policy status.	**show ipfix policy**
Displays online user information.	**show ipfix online** [**user** *user-name* | **ip** *ip-addr* | **count**]

21 Configuring APP-AUTH

21.1 Overview

Conventional Web authentication is based on Remote Authentication Dial In User Service (RADIUS), and the authentication and delivery process is complex. APP-AUTH provides an HTTP-based open and lightweight interactive authentication method. Working over the WiFiDog protocol that is similar to the Linux standard, APP-AUTH can interconnect with the FS business and marketing platform (WMC/MCP) to implement authentication based on short messages, fixed accounts, and WiFi connection over WeChat.

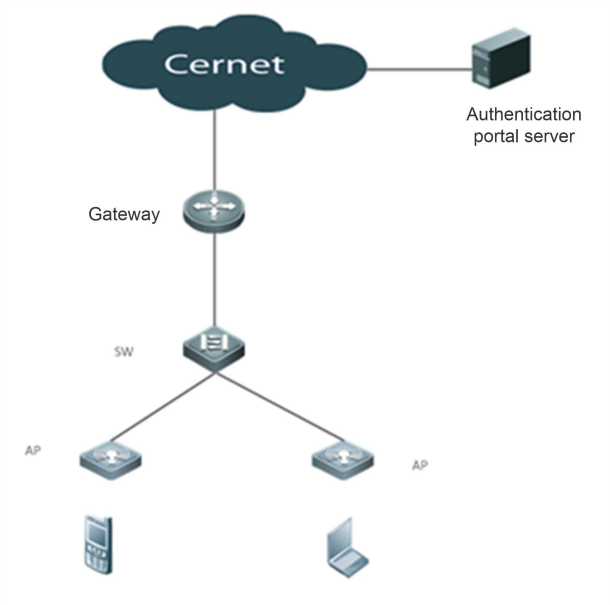
21.2 Applications

Application	Description
Applying APP-AUTH	Describes the typical application of APP-AUTH.

21.2.1 Applying APP-AUTH

Scenario

As shown in the following figure, a mobile client is successfully authenticated by an authentication server and accesses a network via a gateway.



Remarks	The authentication server can be a FS WMC or MCP, or a third-party server that complies with an authentication protocol of APP-AUTH.

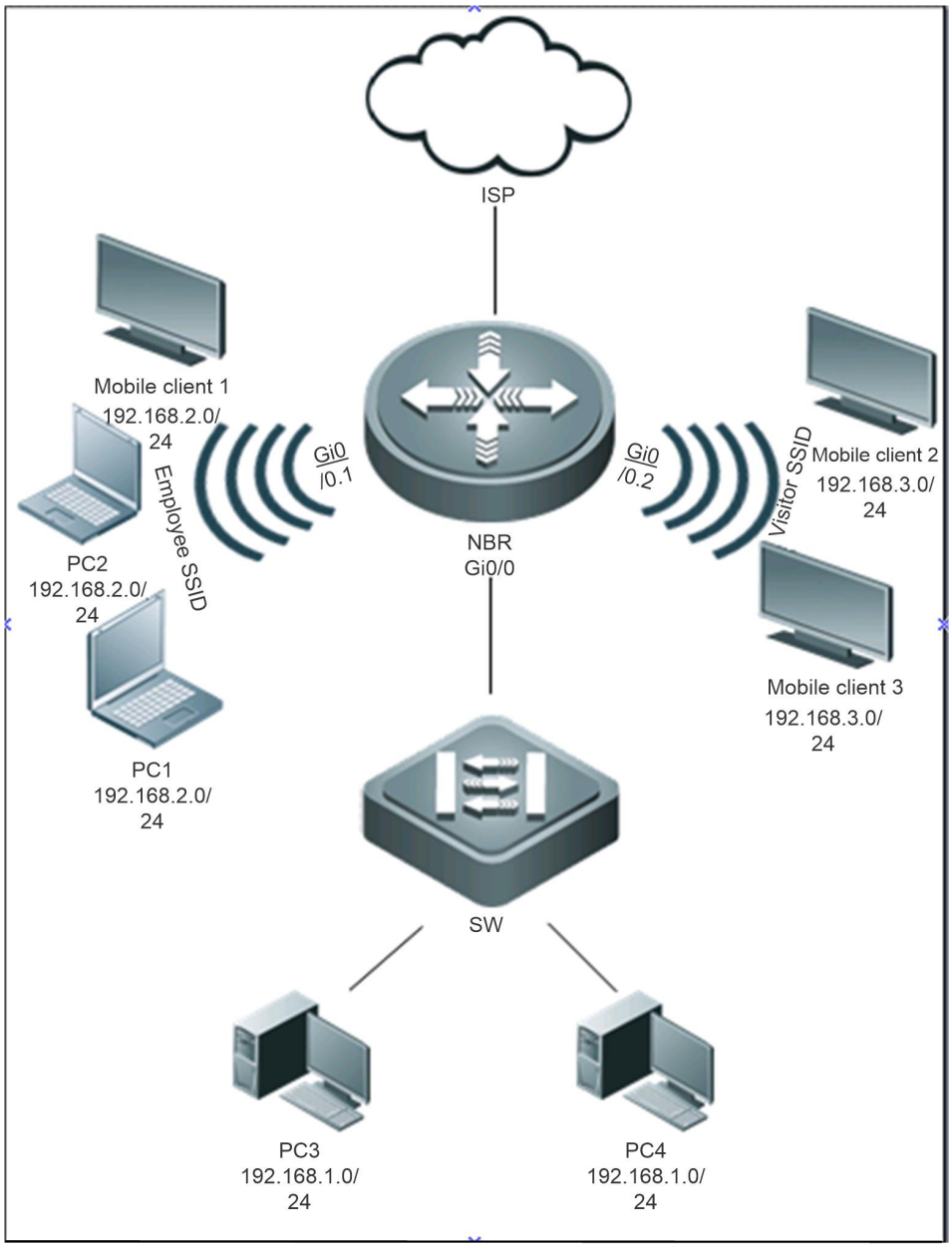
Deployment

- Deploy WiFiDog on the gateway and authentication server for authentication.
- Deploy WiFi connection over WeChat on the gateway and authentication server for authentication.

21.2.2 Local Authentication

Scenario

As shown in the figure below, mobile clients access the public network through the gateway and the authentication is completed by the gateway.



Remarks	No external authentication server is required.

Deployment

- Deploy local authentication on the gateway.

21.3 Features

Basic Concepts

Authentication-free application

Generally, a client cannot access a network without authentication. By configuring an authentication-free application, the client can directly access the network via the application without authentication. Authentication applications indicate the category of applications defined in the application identification signatures database.

WiFiDog

WiFiDog is a token-based security authentication protocol recommended by Linux. This protocol implements communication over HTTP. The gateway WiFiDog is developed by adding relevant device information on the Linux basis.

WiFi connection over WeChat

WiFi connection over WeChat is an open authentication protocol released by WeChat. Users can quickly complete authentication over WeChat, without entering the username, password, or other information. With this protocol, functions such as resident advertisements and WeChat can be implemented.

Authentication policy

Currently, authentication policies are mainly applied in APP-AUTH local authentication scenarios. Different authentication policies can be configured to cater to different user requirements.

User group

Different user groups have different permissions.

User

A user can belong to any user group.

Overview

Feature	Description
WiFiDog-based Authentication	The gateway implements interactive authentication together with the authentication server over WiFiDog.
WiFi Connection over WeChat	The gateway implements interactive authentication together with the authentication server by WiFi connection over WeChat.
Local Authentication	The gateway serves as an authentication server to conduct authentication.

21.3.1 WiFiDog-based Authentication

Working Principle

WiFiDog, similar to the Linux standard, ensures authentication protocol security via tokens. The protocol provides only an authentication method, which is specifically implemented through short messages or fixed accounts. The specific authentication manner is controlled via the authentication server.

Related Configuration

Enabling APP-AUTH

Run the **app-auth enable, app-auth cwmp enable** command in global configuration mode to enable APP-AUTH.

Configuring WiFiDog

WiFiDog is not configured by default.

Run the **app-auth cfg-opt rdt-for-wifidog** command to set the redirection method to WiFiDog.

Run the **app-auth ad-ur**l url command to configure a URL to be redirected to.

Run the **webservice server-ur**l url command to configure a URL for token verification.

21.3.2 WiFi Connection over WeChat

Working Principle

WiFi connection over WeChat is an open authentication protocol released by WeChat. Users can quickly complete authentication over WeChat, without entering the username, password, or other information. With this protocol, functions such as resident advertisements and WeChat can be implemented. The working principle of WiFi connection over WeChat is similar to that of WiFiDog, but the token verification is performed by the WeChat server.

Related Configuration

Enabling APP-AUTH

Run the **app-auth enable, app-auth cwmp enable** command in global configuration mode to enable APP-AUTH.

Configuring WiFi Connection over WeChat

WiFi connection over WeChat is not configured by default.

Run the **app-auth cfg-opt rdt-for-wx2** command to set the redirection method to WiFi connection over WeChat.

Run the **app-auth ad-url** *url* command to configure a URL to be redirected to.

Run the **webservice server-url** *url* command to configure the URL of the server.

21.3.3 Local Authentication

Working Principle

The gateway serves as an authentication server and pushes different authentication pages to users based on user requirements, to complete authentication of different users.

Related Configuration

Enabling Local Authentication

Local authentication needs to be enabled globally. Run the **app-auth local-auth enable** command to enable local authentication.

Configuring an Authentication Policy

No authentication policy is configured by default.

Run the **app-auth policy** command to configure an authentication policy.

Configuring a VIP User Group

No VIP user group is configured by default.

Run the **app-auth local-auth vip-group** command to configure a VIP user group.

Configuring a User

No user is configured by default.

Run the **app-auth local-auth subs-name** command to configure a user.

21.4 Configuration

Configuration	Description and Command	
Configuring General Switch	(Optional) It is used to enable APP-AUTH in global configuration mode.	
	app-auth enable	Enables APP-AUTH in global configuration mode.
	app-auth cwmp enable	Enables the server correlation function.
Configuring Redirection Method	(Optional) It is used to select a redirection method according to the protocol.	
	app-auth cfg-opt rdt-for-wifidog	Sets the redirection method to WiFiDog.
	app-auth cfg-opt rdt-for-wx2	Sets the redirection method to WiFi connection over WeChat.
Configuring URL to Be Redirected to	Optional	
	app-auth ad-url	Configures a portal URL to be redirected to.
Configuring Authentication-free Applications	(Optional) It is used to allow users to directly access an extranet without authentication.	
	app-auth direct-app *app-name*	Configures authentication-free applications.
Configuring Network Segment	(Optional) It is used to authenticate clients of all network segments by default when APP-AUTH is enabled. After a network segment is configured, only clients in the configured network segment will be authenticated.	
	app-auth auth-url ip start end	Configures a network segment.

Configuring Authentication-free IP Address Range in Intranet	(Optional) It is used to enable clients within the IP address range to directly access all network resources.	
	app-auth direct-srcip *ip_start* **[** *ip_end* **]** **[aging-time** *time* **] [comment** *string* **]**	Configures an authentication-free IP address range in the intranet.
Configuring Authentication-free Extranet Resource Range	(Optional) It is used to enable clients to directly access extranet resources within the IP address range before authentication.	
	app-auth direct-dstip *ip_start* **[** *ip_end* **]** **[aging-time** *time* **] [comment** *string* **]**	Configures an authentication-free extranet resource range.
Configuring URL Whitelist	(Optional) It is used to allow requests corresponding to the URLs. Wildcards are supported.	
	app-auth direct-url url	Configures URLs corresponding to which requests are allowed.
Configuring Intranet MAC Address Whitelist	(Optional) It is used to enable clients in the MAC address whitelist to access network resources without authentication.	
	app-auth direct-mac mac **[aging-time** *time* **] [comment** *string* **]**	Configures an intranet MAC address whitelist.
Configuring Intranet MAC Address Blacklist	(Optional) It is used to forbid clients in the MAC address blacklist to access network resources.	
	app-auth deny-mac mac **[aging-time** *time* **] [comment** *string* **]**	Configures an intranet MAC address blacklist.
Configuring Traffic Monitoring Result as Basis for Client Go-offline	(Optional) It is used to force clients with traffic less than the specified limit within a period to go offline.	
	app-auth offline-detect [time-interval *time* **flowrate** *flow* **]**	Configures traffic monitoring result as a basis for client go-offline.
Configuring Private Information of Redirection	(Optional) It is used for customized clients.	
	app-auth priv-info info	Configures private information of redirection.
Configuring Network Type	(Optional) It is used to select a network type according to the network topology.	
	app-auth cfg-opt [id-mac | id-ip]	Configures a network type.
Configuring Network Segments and SSIDs	(Optional) It is used to enable SSIDs to correspond to different network segments.	
	app-auth set-ssid ssid-name **{ ip-range** ip-start ip-end**}**	Configures network segments and SSIDs.
Configuring TCP Keepalive Connections	Optional	
	app-auth tcp-socket [**enable / server** *server-url* / **keepalive** *time_1* / **user-inform** *time_2*]	Configures TCP keepalive connections.

Deleting Online Clients	It is used to delete online clients.	
	app-auth kick all	Deletes all online clients.
	app-auth kick ip *ip-addr*	Deletes online clients with specified IP addresses.
Enabling Local Authentication Globally	Optional.	
	app-auth local-auth enable	Enables local authentication globally.
Configuring a Locally Authenticated User	Optional.	
	app-auth local-auth subs-name *name* **type** { **ad** | **local** }	Configures a locally authenticated user.
Configuring Client Information of a Locally Authenticated User	Optional.	
	mac *mac-address* { **auto** | **manual** } **type** { **pc** | **mobile** }	Configures client information of a locally authenticated user.
Configuring the Upper Limit of Clients That Can Be Used by Each Locally Authenticated User	Optional.	
	app-auth local-auth subscriber mac-limit *limit-num*	Configures the upper limit of clients that can be used by each locally authenticated user.
Configuring Automatic Account Binding for Locally Authenticated Users	Optional.	
	app-auth local-auth data-store enable	Configures automatic account binding for locally authenticated users.
Configuring Automatic Aging Time of Information About Locally Authenticated Users in the Database	Optional.	
	app-auth local-auth data-store age day *day*	Configures automatic aging time of information about locally authenticated users in the database.
Configuring an Authentication Server	Optional.	
	app-auth server *name* **type** { **act-directory** | **qrcode-alone** | **qrcode-authorize** | **sms** | **weixin** }	Configures an authentication server.
Configuring an IP Address for Accessing the QR Code	Optional.	
	local-auth qrcode ip *ip-address*	Configures an IP address for accessing the QR code.
Configuring a Dynamic Code for the QR Code	Optional.	
	local-auth qrcode key *key-str*	Configures a dynamic code for the QR code.
Configuring a	Optional.	

Comment on the QR Code	**local-auth qrcode comment** *comment-str*	Configures a comment on the QR code.
Configuring Parameters Related to QR Code Authorization-based Authentication	Optional.	
	app-auth local-auth { **authorize** { **check** | **restrict-times** *times* } | **authorize-time** *minute* }	Configures parameters related to QR code authorization-based authentication.
Configuring Parameters of the SMS Server	Optional.	
	local-auth sms keyid *keyid-str* **keysecret** *keysecret-str* **sign** *sign-str* **templet** *templet-str*	Configures parameters of the SMS server.
Configuring the Type of the SMS Server	Optional.	
	local-auth sms server { **aliyun-v1** | **aliyun-v2** }	Configures the type of the SMS server.
Configuring the Mobile Phone Prior Mode in SMS-based Authentication	Optional.	
	local-auth sms mode prior	Configures the mobile phone prior mode.
Configuring Parameters Related to WeChat-based Authentication	Optional.	
	local-auth weixin shopid *shopid-str* **appid** *appid-str* **secretkey** *secretkey-str*	Configures parameters related to WeChat-based authentication.
Configuring the SSID of the Authentication Server	Optional.	
	local-auth weixin ssid *ssid-str*	Configures the SSID of the authentication server.
Configuring an Authentication Policy Group	Optional.	
	app-auth policy *name*	Configures an authentication policy group.
Enabling This Authentication Policy	Optional.	
	rule enable	Enables this authentication policy.
Configuring an IP Address Range in Which an Authentication Policy Is Effective	Optional.	
	rule ip-range { [*ip1* { *ip2* }] | **all** }	Configures an IP address range in which an authentication policy is effective.
Configuring an	Optional.	

Authentication Server Associated with an Authentication Policy	**relate server** *server-name*	Configures an authentication server associated with an authentication policy.
Configuring the Authentication Type of an Authentication Policy	Optional.	
	rule type pwd	Configures the authentication type of an authentication policy.
Configuring the Available Online Duration for Local Users Who Are Successfully Authenticated	Optional.	
	app-auth local-auth online-time *time*	Configures the available online duration for local users who are successfully authenticated.
Restricting Clients in Specific Types from Internet Access	Optional.	
	app-auth local-auth restrict { **pc** | **mobile** } [**exclude time-range** *time*]	Restricts clients in specific types from Internet access.

21.4.1 Configuring General Switch

Configuration Effect

- Enable APP-AUTH in global configuration mode. After the function is enabled, configurations related to APP-AUTH will take effect.

Configuration Steps

- Configure the general switch to enable APP-AUTH.

Verification

- Check whether clients can access networks before the function is enabled.
- Check whether clients can access networks after the function is enabled.

Related Commands

Enabling APP-AUTH

Command	app-auth enable
Parameter Description	
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling External Authentication Function

Command	**app-auth cwmp enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure this command together with the **app-auth enable** command.

Configuration Example

Enabling APP-AUTH

Configuration Steps	Enable APP-AUTH on the gateway.
	FS# configure terminal FS(config)# app-auth enable FS(config)# app-auth cwmp enable
Verification	Run the **show app-auth statistic** command to display the configuration result. FS#show app-auth statistics ----------start---------- app_auth_enable: on cwmp_enable: on cwmp_bak: off non_http_pass: off device_serialno: 1234942571228 basename: 401034050039 portal_key: g_wan_ip: 0.0.0.0 priv_info: siteid=fs time_limit: 0 server_status: 1 app_webs_sin_ip: 0.0.0.0 flow_detect status: on flow_detect time_interval: 60 (min) flow_detect flowrate: 0 (bit/s) flow_detect detect_limit: 120 advertising_url:

```
avoid app_name:
          sina microblog (1-6-1-0)
auth app_name:
          IM(0-0-0-0)
auth_url:
          http://www.fs.com.cn


distri msg. up: 0, down: 0, inq: 0, attent:0
rcv_msg_num: 585, rcv_query_msg_num: 0
---------------------------------end-------------------------------
```

When app_auth_enable and cwmp enable are on means start

21.4.2 Configuring Redirection Method

Configuration Effect

- Carry different parameters according to the redirection method configured.

Configuration Steps

- Optional.
- Configure a redirection method according to the selected protocol.

Verification

- View the URL of the portal page to verify that different parameters are carried according to the redirection method configured.

Related Commands

Setting Authentication Method to WiFiDog

Command	**app-auth cfg-opt rdt-for-wifidog**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use command when WiFiDog is configured.

Setting Authentication Method to WiFi Connection over WeChat

Command	**app-auth cfg-opt rdt-for-wx2**
Parameter Description	**N/A**
Command Mode	Global configuration mode

Usage Guide	Use command when WiFi connection over WeChat is configured.

Configuration Example

Setting Redirection Method to WiFiDog

Configuration Steps	
	FS# configure terminal FS(config)# app-auth cfg-opt rdt-for-wifidog
Verification	Run the **show app-auth cfg-opt** command to display the configuration result.

21.4.3 Configuring URL to Be Redirected to

Configuration Effect

- Redirect clients that intend to access any website using a browser before authentication to this URL.

Notes

- The configuration method and redirection method must be negotiated with the server in advance.

Configuration Steps

- Optional.
- Configure a URL according to the specific server.

Verification

- Verify that clients that intend to access any website using a browser before authentication are redirected to this URL.

Related Commands

Configuring URL to Be Redirected to

Command	**app-auth ad-url** *string*
Parameter Description	*String*: Indicates a URL to be redirected to.
Command Mode	Global configuration mode
Usage Guide	Before authentication, advertisement URLs are pushed to the clients. During URL configuration, the prefix "http://" is dispensable.

Configuration Example

Configuring URL to Be Redirected to as http://wmc.fsyun.com and Setting Redirection Method to WiFiDog

Configuration Steps	
	FS# configure terminal FS(config)# app-auth ad-url http://wmc.fsyun.com FS(config)# app-auth cfg-opt rdt-for-wifidog
Verification	Verify that clients that intend to access http://www.qq.com using a browser are redirected to http://wmc.fsyun.com.

Common Errors

- No corresponding function is configured for the server. As a result, the portal page cannot be displayed.
- The IP address of the server is not added to the authentication-free range.

21.4.4 Configuring Authentication-free Applications

Configuration Effect

- Enable clients to directly use authentication-free applications without authentication.

Notes

- The configured authentication-free applications must exist in the application identification signatures database.

Configuration Steps

- Optional.

Verification

- Run the show app-auth statistics command.

Related Commands

Configuring Authentication-free Applications

Command	app-auth direct-app *app-name*
Parameter Description	*app-name:* Indicates an application name.
Command Mode	Global configuration mode
Usage Guide	Use this command to directly allow clients based on applications.

Configuration Example

Configuring Sina Microblog as Authentication-free Application

Configuration Steps	Configure an authentication-free application.
	FS (config)# app-auth direct-app *Sina Microblog*
Verification	Run the **show app-auth statistics** command to display the configuration result.

```
-----------------------------start--------------------------------
app_auth_enable: on
cwmp_enable: off
cwmp_bak: off
non_http_pass: off
device_serialno: 1234942571228
basename: 401034050039
portal_key:
g_wan_ip: 0.0.0.0
priv_info: siteid=fs
time_limit: 0
server_status: 1
app_webs_sin_ip: 0.0.0.0
flow_detect status: on
        flow_detect time_interval: 60 (min)
        flow_detect flowrate: 0 (bit/s)
        flow_detect detect_limit: 120
advertising_url:
avoid app_name:
        sina microblog (1-6-1-0)
auth app_name:
auth_url:
        http://www.fs.com.cn

distri msg. up: 0, down: 0, inq: 0, attent:0
rcv_msg_num: 2842, rcv_query_msg_num: 0
---------------------------------end-------------------------------
```

Common Errors

- The configured authentication-free application does not exist in the application identification signatures database.

21.4.5 Configuring Network Segment

Configuration Effect

- Enable only clients within the configured network segment to be authenticated by using the APP-AUTH function.

Configuration Steps

- Optional.

Verification

- Verify that only clients within the configured network segment are authenticated by using the APP-AUTH function, and that other clients can directly access networks.

Related Commands

Configuring Network Segment

Command	**app-auth auth-rule** { { **ip** start end } | { **ipv6** *start end* } }
Parameter Description	*start*: Indicates the start IPv4/v6 address. *end*: Indicates the end IPv4/v6 address.
Command Mode	Global configuration mode
Usage Guide	Use this command when the Web authentication function is enabled.

Configuration Example

Configuring 192.168.1.0/24 as Network Segment to Be Authenticated

Configuration Steps	Configure a network segment to be authenticated.
	FS (config)# app-auth auth-rule ip 192.168.1.1 192.168.1.255
Verification	Run the **show app-auth auth-rule** command to display the configuration result. FS(config)#show app-auth auth-rule auth-rule ip: 192.168.10.2 - 192.168.10.100 Verify that the clients within the IP address range can be successfully authenticated before they access network resources.

21.4.6 Configuring Authentication-free IP Address Range in Intranet

Configuration Effect

- Enable clients with the IP addresses in the authentication-free IP address range to directly access all reachable network resources without authentication.
- No authentication-free IP address range is configured by default.

Configuration Steps

- Optional.
- Configure the authentication-free IP address range so that corresponding clients can access the network without authentication.

Verification

- Configure an authentication-free IP address range.
- Verify that clients with the IP addresses in the authentication-free IP address range can directly access network resources.

Related Commands

Configuring Authentication-free IP Address Range

Command	**app-auth direct-srcip** { { *ip_start* [*ip_end*] } | { *ipv6_start* [*_ipv6_end*] } } [**aging-time** *time*] [**comment** *string*]
Parameter Description	*ip_start*: Indicates the start IPv4 address of authentication-free clients. *ip_end*: Indicates the end IPv4 address of authentication-free clients. *ipv6_start*: Indicates the start IPv6 address of authentication-free clients. *ipv6_end*: Indicates the end IPv6 address of authentication-free clients. *time*: Indicates the aging time. *string*: Describes this configuration.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring Authentication-free IP Address Range

Configuration Steps	Configure an authentication-free IP address range.
	FS (config)# app-auth direct-srcip 192.168.10.2 192.168.10.100
Verification	Run the **show app-auth direct-srcip** command to display the configuration result. FS(config)#show app-auth direct-srcip direct src-ip: 192.168.10.2 - 192.168.10.100 Verify that the clients within the IP address range can be successfully authenticated before they

	access network resources.

21.4.7 Configuring Authentication-free Extranet Resource Range

Configuration Effect

- Enable clients to directly access extranet resources within the authentication-free IP address range before authentication.

Configuration Steps

- Optional.
- Configure an authentication-free IP address range to allow clients to access corresponding network resources before authentication.

Verification

- Verify that clients can access network resources within the authentication-free IP address range without authentication.

Related Commands

Configuring Authentication-free Extranet Resource Range

Command	**app-auth direct-dstip** { { *ip_start* [*ip_end*] } | { *ipv6_start* [*ipv6_end*] } } [**aging-time** *time*] [**comment** *string*]
Parameter Description	*ip_start*: Indicates the start IPv4 address of the network resource range that can be directly accessed by clients. *ip_end*: Indicates the end IPv4 address of the network resource range that can be directly accessed by clients. *ipv6_start*: Indicates the start IPv6 address of the network resource range that can be directly accessed by clients. *ipv6_end*: Indicates the end IPv6 address of the network resource range that can be directly accessed by clients. *time*: Indicates the aging time. *string*: Describes this configuration.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring www.baidu.com as Authentication-free URL

Configuration Steps	Run the **ping www.baidu.com** command to obtain the IP address 115.239.210.27.
	FS (config)# app-auth direct-dstip 115.239.210.27

Verification	Run the **show app-auth direct-dstip** command to display the configuration result. FS(config)#show app-auth direct-dstip direct dst-ip: 115.239.210.27 Verify that clients can access http://115.239.210.27 to open the homepage of Baidu without authentication.

21.4.8 Configuring URL Whitelist

Configuration Effect

- Enable clients to directly access URLs in the whitelist without authentication.

Notes

- Wildcards are supported. For example, if baidu.com is in the whitelist, both www.baidu.com and news.baidu.com can be accessed.
- If an access request corresponding to the URL is encrypted, the corresponding client must send a DNS request. In this case, whitelist validation may be delayed.

Configuration Steps

- Optional.

Verification

- Verify that clients can directly access URLs in the whitelist without authentication.

Related Commands

Configuring Authentication-free URL Whitelist

Command	**app-auth direct-url** *url*
Parameter Description	*url*: Indicates a URL whitelist.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Adding fs.com.cn into URL Whitelist

Configuration Steps	Add fs.com.cn into the URL whitelist.
	FS (config)# app-auth direct-url fs.com.cn

Verification	Run the **show app-auth direct-url** command to display the configuration result. FS(config)#show app-auth direct-url direct url: fs.com.cn Verify that clients can access fs.com.cn without authentication.

21.4.9 Configuring Intranet MAC Address Whitelist

Configuration Effect

- Enable clients in the MAC address whitelist to access networks without authentication.

Notes

- This function takes effect on the L2 network.

Configuration Steps

- Optional.
- Configure a MAC address whitelist to enable authentication-free access of specified clients.

Verification

- Verify that clients in the MAC address whitelist can access network resources without authentication.

Related Commands

Configuring MAC Address Whitelist

Command	**app-auth direct-mac** *mac-address* [**aging-time** *time*] [**comment** *string*]
Parameter Description	*mac-address*: Indicates a MAC address. *time*: Indicates the aging time. *string*: Describes this configuration.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring Intranet MAC Address Whitelist

Configuration Steps	Add the MAC address 78f5.df63.b014 into the whitelist.
	FS (config)# app-auth direct-mac 78f5.df63.b014
Verification	Run the **show app-auth direct-mac** command to display the configuration result.

	FS#show app-auth direct-mac app-auth direct-mac num: 1 mac: 78f5.df63.b014, flag: 0 Verify that the client with the MAC address can access network resources without authentication.

21.4.10 Configuring Intranet MAC Address Blacklist

Configuration Effect

- Forbid clients in the MAC address blacklist to be authenticated or access network resources.

Notes

- This function takes effect on the L2 network.

Configuration Steps

- Optional.
- Configure a MAC address blacklist to forbid network access of specified clients.

Verification

- Verify that clients in the MAC address blacklist cannot access network resources.

Related Commands

Configuring MAC Address Blacklist

Command	**app-auth deny-mac** *mac-address* [**aging-time** *time*] [**comment** *string*]
Parameter Description	*mac-address*: Indicates a MAC address. *time*: Indicates the aging time. *string*: Describes this configuration.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring Intranet MAC Address Blacklist

Configuration Steps	Add the MAC address d014.df63.b014 into the blacklist.
	FS (config)# app-auth deny-mac d014.df63.b014
Verification	Run the **show app-auth deny-mac** command to display the configuration result. FS(config)#show app-auth deny-mac

	app-auth deny-mac num: 1 mac: d014.df63.b014, flag: 1 Verify that the client with the MAC address cannot be authenticated or access network resources.

21.4.11 Configuring Traffic Monitoring Result as Basis for Client Go-offline

Configuration Effect

- Enable clients with traffic less than the specified limit within a period to automatically go offline.

Notes

- The period must be less than a half of the DHCP cycle.

Configuration Steps

- Optional.
- Enable this function to recycle IP addresses of clients whose traffic is less than the specified limit.

Verification

- Verify that clients with traffic less than the specified limit within a period automatically go offline.

Related Commands

↘ Configuring Traffic Monitoring Result as Basis of Client Go-offline

Command	**app-auth offline-detect [time-interval t*ime* flowrate *flow]***
Parameter Description	*time*: Indicates the monitoring time in the unit of minute. The value ranges from 1 to 65,535. The default value is 15. *flow*: Indicates a traffic limit in the unit of bps. A client with traffic reaching the limit automatically goes offline. The default value is 0.
Command Mode	Global configuration mode
Usage Guide	N/A

21.4.12 Configuring Private Information of Redirection

Configuration Effect

- Enable the URL redirection message to carry private information after the information is configured.

Notes

- This function is configured if a customer expects a URL redirection message to carry additional information.

Configuration Steps

- Optional.

Related Commands

Configuring Private Information of Redirection

Command	**app-auth priv-info** *info*
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Negotiate with the customer about the private information to be carried.

21.4.13 Configuring Network Type

Configuration Effect

- Configure a network type according to the network topology (L2 or L3). If L2 is selected, uniquely identify a client by a MAC address on the egress gateway. If L3 is selected, uniquely identify a client by an IP address on the egress gateway.

Notes

- A network type is selected according to the network topology. If a network topology is unknown, select L3.
- After a network type is changed, run the **app-auth kick all** command to delete all clients. The clients need to be re-authenticated.

Configuration Steps

- Optional.

Verification

- Run the show app-auth cfg-optt command.

Related Commands

Configuring L2 Network Type

Command	**app-auth cfg-opt id-mac**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command when the network topology must be set to L2.

Configuring L3 Network Type

Command	**app-auth cfg-opt id-ip**
Parameter	N/A

Description	
Command Mode	Global configuration mode
Usage Guide	Use this command when the network topology can be set to L2 or L3.

Common Errors

21.4.14 Configuring Network Segments and SSIDs

Configuration Effect

- Match the client IP address with a network segment after the network segment is configured. If an IP address is matched, enable the gateway to carry the SSID during redirection.

Notes

- This function is configured when it is confirmed that the servers need and support SSIDs.
- A global SSID can be configured.

Configuration Steps

- Optional.

Verification

- Run the show app-auth ssid-cfg command.

Related Commands

↘ Configuring Network Segments and SSIDs

Command	**app-auth set-ssid** ssid-name { **ip-range** ip-start ip-end}
Parameter Description	*ssid-name*: Indicates the SSID name. *ip-start*: Indicates the start IPv4 address. *ip-end*: Indicates the end IPv4 address.
Command Mode	Global configuration mode
Usage Guide	1. If no network segment is configured, configure a global SSID. 2. Ensure that the SSID of a network segment takes priority over a global SSID.

Common Errors

- The configured SSID name is inconsistent with that of the actual SSID, for example, the SSID configured on the AC.

21.4.15 Configuring TCP Keepalive Connections

Configuration Effect

- Ensure that the gateway and server maintain a TCP keepalive connection over which client synchronization and status advertisement can be implemented.

Notes

- The server must support the function. Generally, the function is used for authentication and accounting.

Configuration Steps

- Optional.

Verification

- Run the show app-auth tcp-info command.

Related Commands

Configuring TCP Keepalive Connections

Command	**app-auth tcp-socket** [***enable*** / ***server*** *server-url* / ***keepalive*** *time_1* / ***user-inform*** *time_2*]
Parameter Description	*enable*: Enables a TCP keepalive connection. *server-url*: Indicates a server IP address. *time_1*: Specifies a TCP keepalive period. The default value is 30 seconds. *time_2*: Specifies a client synchronization period. The default value is five minutes.
Command Mode	Global configuration mode
Usage Guide	Use this command when the servers support this function. Generally, use this function for authentication and accounting.

21.4.16 Deleting Online Clients

Configuration Effect

- Ensure that deleted online clients cannot access network resources.

Configuration Steps

- Optional.

Related Commands

Deleting All Online Clients

Command	**app-auth kick all**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Deleting Online Clients with Specified IP Addresses

Command	**app-auth kick** { { **ip** *ip-addr* }

Parameter Description	*ip-addr*: Indicates an IPv4 address of an online client.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

21.4.17 Configuring HTTPS Re-direction

Configuration Effect

- Re-direct HTTPS traffic.

Configuration Steps

- Optional.

Verification

- Run the **show app-auth proxy-option config** command to display the configuration status.

Related Commands

Configuring HTTPS Re-direction

Command	**app-auth proxy-option [https | session total** *total-num* **per-ip** *per-ip-num* **]**
Parameter Description	**session total** *total-num*: Indicates the limit on the total number of HTTPS sessions in the entire system. **per-ip** *per-ip-num*: Indicates the limit on the number of HTTPS sessions for each IP address. **https**: Enables HTTPS re-direction.
Command Mode	Global configuration mode
Usage Guide	After authentication is enabled, HTTPS re-direction is effective only to offline clients.

21.4.18 Enabling Local Authentication Globally

Configuration Effect

- Enable the local authentication mode.

Notes

- This configuration is used for local authentication only.

Configuration Steps

- Optional.

Verification

- Run the **show app-auth local-auth config** command to display the configuration.

Related Commands

Enabling Local Authentication

Command	**app-auth local-auth enable**
Parameter Description	**enable**: Enables local authentication.
Command Mode	Global configuration mode
Usage Guide	Use this command in local authentication scenarios.

Configuration Example

Enabling Local Authentication

Configuration Steps	● Enable local authentication on the gateway.
	FS# configure terminal FS(config)# app-auth local-auth enable
Verification	● Run the **show app-auth local-auth config** command to check whether the function is enabled. FS#show app-auth local-auth config app-auth local-auth enable

Common Errors

- N/A

21.4.19 Configuring a Locally Authenticated User

Configuration Effect

- Configure information about a locally authenticated user.

Notes

- This configuration is used for local authentication only.

Configuration Steps

- Optional.

Verification

- Run the **show app-auth local-auth subs** command to display the configuration.

Related Commands

Configuring a Locally Authenticated User

Command	**app-auth local-auth subs-name** *name* **type local**

Parameter Description	*name*: Indicates a username. **local:** Indicates a local user.
Command Mode	Global configuration mode
Usage Guide	The configured user is valid only in LOCAL-AUTH.

Configuration Example

Configuring a Locally Authenticated User

Configuration Steps	● Configure locally authenticated user named abc on the gateway and set the user type to AD.
	FS# configure terminal FS(config)# app-auth local-auth subs-name abc type ad
Verification	● Run the **show app-auth local-auth subs all** command to display information about the locally authenticated user. FS# show app-auth local-auth subs all subs_cnt:1/1200, mac_cnt: 1/2500 ---------- Name Mac_num Type source Mode Mac Auto/Manual terminal time ---------- abc 1 ad ad manual |---- 0011.2233.4455 manual pc 2018-5-18 16:42:13

Common Errors

- Locally authenticated users are independent from users configured on the user management module and they do not affect each other.

21.4.20 Configuring Client Information of a Locally Authenticated User

Configuration Effect

- Configure client information of a locally authenticated user.

Notes

- This configuration is used for local authentication only.

Configuration Steps

- Optional.

Verification

- Run the **show app-auth local-auth subs** command to display the configuration.

Related Commands

Configuring Client Information of a Locally Authenticated User

Command	**mac** *mac-address* { **auto** | **manual** } **type** { **pc** | **mobile** }
Parameter Description	**mac**: Indicates the MAC address of a client. *mac-address*: Specifies the MAC address in the xxxx.xxxx.xxxx format. **auto**: Indicates that the client information is automatically imported. **manual**: Indicates that the client information is manually configured. **pc**: Indicates that the client is a PC. **mobile**: Indicates that the client is a mobile device.
Command Mode	APP-AUTH user configuration mode
Usage Guide	This configuration is effective only to local authentication. Multiple clients can be configured for one user.

Configuration Example

Configuring Client Information of a Locally Authenticated User

Configuration Steps	- Configure locally authenticated user named abc on the gateway, set the user type to AD, client type to PC, and MAC address to 0011.2233.4455.
	FS# configure terminal FS(config)# app-auth local-auth subs-name abc type ad FS(config)# mac 0011.2233.4455 manual type pc
Verification	- Run the **show app-auth local-auth subs all** command to display information about the locally authenticated user. FS# show app-auth local-auth subs all subs_cnt:1/1200, mac_cnt: 1/2500 ---------- Name Mac_num Type source Mode Mac Auto/Manual terminal time ---------- abc 1 ad

	ad manual |---- 0011.2233.4455 manual pc 2018-5-18 16:42:13

Common Errors

- Locally authenticated users are independent from users configured on the user management module and they do not affect each other.

21.4.21 Configuring a VIP User

Configuration Effect

- VIP users can assign the Internet access permission to other users when the authorized management and control is enabled.

Notes

- This configuration is used for local authentication only.

Configuration Steps

- Optional.

Verification

- Run the **show app-auth local-auth vip-group all** command to display the configuration.

Related Commands

Configuring a Locally Authenticated User as a VIP User

Command	**app-auth local-auth vip-group** *user-name* **local**
Parameter Description	**vip-group**: Indicates a VIP group. *user-name*: Indicates a user to be added to the VIP group. **local**: Indicates a local user.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring a Local User as a VIP User

Configuration Steps	• Configure user named aaa as a VIP user.
	FS# configure terminal FS(config)# app-auth local-auth vip-group aaa local

Verification	● Run the **show app-auth local-auth vip-group all** command to display the configuration. FS# show app-auth local-auth vip-group all cnt: 1/100. ad_any_vip: 0 Group-name type idx ---------- aaa local 0

Common Errors

- N/A

21.4.22 Configuring the Upper Limit of Clients That Can Be Used by Each Locally Authenticated User

Configuration Effect

- Configure the upper limit of clients that can be used by each locally authenticated user.

Notes

- This configuration is used for local authentication only.

Configuration Steps

- Optional.

Verification

- Run the **show app-auth local-auth config** command to display the configuration.

Related Commands

↘ Configuring the Upper Limit of Clients That Can Be Used by Each Locally Authenticated User

Command	**app-auth local-auth subscriber mac-limit** *limit-num*
Parameter Description	*limit-num*: Indicates the upper limit. The default value is **0**, indicating no limitation.
Command Mode	Global configuration mode
Usage Guide	For the prevention of excessive user data automatically generated due to network exceptions, it is necessary to restrict the upper limit of clients that can be used by each locally authenticated user.

Configuration Example

↘ Configuring the Upper Limit of Clients That Can Be Used by Each Locally Authenticated User

Configuration Steps	● Set the upper limit of clients that can be used by each locally authenticated user to 5 on

	the gateway.
	FS# configure terminal FS(config)# app-auth local-auth subscriber mac-limit 5
Verification	● Run the **show app-auth local-auth config** command to display the configuration and check the value of **user-mac-limit**. FS#show app-auth local-auth config enable: False data-store-enable: False data-store-age-day: 60 user-mac-limit: 2 online-time: 0 authorize-time: 0 restrict-range information: mobile: global: false name: state: Idle pc: global: false name: state: Idle

Common Errors

- Locally authenticated users are independent from users configured on the user management module and they do not affect each other.

21.4.23 Configuring Automatic Account Binding for Locally Authenticated Users

Configuration Effect

- Configure automatic account binding for locally authenticated users.

Notes

- This configuration is used for local authentication only.

Configuration Steps

- Optional.

Verification

- Run the **show app-auth local-auth config** command to display the configuration.

Related Commands

Configuring Automatic Account Binding for Locally Authenticated Users

Command	**app-auth local-auth data-store enable**
Parameter Description	**Enable**: Enables automatic account binding.
Command Mode	Global configuration mode
Usage Guide	User information is stored in the database after a user is successfully authenticated.

Configuration Example

Configuring Automatic Account Binding for Locally Authenticated Users

Configuration Steps	- Enable automatic account binding for locally authenticated users on the gateway.
	FS# configure terminal FS(config)# app-auth local-auth data-store enable

Verification	- Run the **show app-auth local-auth config** command to display local authentication configuration and check the value of **data-store-enable**.
	FS#show app-auth local-auth config
	enable: False
	data-store-enable: True
	data-store-age-day: 60
	user-mac-limit: 2
	online-time: 0
	authorize-time: 0
	restrict-range information:
	  mobile:
	  global: false
	  name:
	  state: Idle
	  pc:

	global: false name: state: Idle

Common Errors

- N/A

21.4.24 Configuring Automatic Aging Time of Information About Locally Authenticated Users in the Database

Configuration Effect

- Configure automatic aging time of information about locally authenticated users in the database.

Notes

- This configuration is used for local authentication only.

Configuration Steps

- Optional.

Verification

- Run the **show app-auth local-auth config** command to display the configuration.

Related Commands

↘ Configuring Automatic Aging Time of Information About Locally Authenticated Users in the Database

Command	**app-auth local-auth data-store age day** *day*
Parameter Description	*day:* Indicates the aging period.
Command Mode	Global configuration mode
Usage Guide	User information in the user database automatically ages. When the aging period expires, data stored in the user database is deleted.

Configuration Example

↘ Configuring Automatic Aging Time of Information About Locally Authenticated Users in the User Database

Configuration Steps	● Set the automatic aging period of information about locally authenticated users to 5 days on the gateway.
	FS# configure terminal FS(config)# app-auth local-auth data-store age day 5

Verification	● Run the **show app-auth local-auth config** command to display the local authentication configuration and check the value of **data-store-age-day**.
	FS#show app-auth local-auth config
	enable: False
	data-store-enable: True
	data-store-age-day: 5
	user-mac-limit: 2
	online-time: 0
	authorize-time: 0
	restrict-range information:
	  mobile:
	  global: false
	  name:
	  state: Idle
	  pc:
	  global: false
	  name:
	  state: Idle

Common Errors

- N/A

21.4.25 Configuring an Authentication Server

Configuration Effect

- Configure an authentication server.

Notes

- N/A

Configuration Steps

- Optional.

Verification

- Run the **show app-auth policy** command to display the configuration.

Related Commands

Configuring an Authentication Server

Command	**app-auth server** *name* **type** { **qrcode-alone** | **qrcode-authorize** | **sms** | **weixin** }
Parameter Description	*name*: Indicates the server name. **qrcode-alone**: Indicates authentication based on self-help QR code scanning. **qrcode-authorize**: Indicates authentication based on authorized QR code scanning. **sms**: Indicates SMS-based authentication. **weixin**: Indicates WeChat-based authentication.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure an authentication server.

Configuration Example

Configuring an Authentication Server

Configuration Steps	● Configure authentication server named abc on the gateway and set the authentication mode to **qrcode-alone**.
	FS# configure terminal FS(config)# app-auth server abc type qrcode-alone
Verification	● Run the **show app-auth policy** command to display the authentication server configuration. FS# show app-auth server all server name: abc type: qrcode-alone mode: alone comment: Welcome! ip: 2.2.2.2 key: 1

Common Errors

- N/A

21.4.26 Configuring an IP Address for Accessing the QR Code

Configuration Effect

- Users can access the QR code through this IP address.

Notes

- N/A

Configuration Steps

- Optional.

Verification

- Run the **show app-auth server all** command to display the configuration.

Related Commands

Configuring an IP Address for Accessing the QR Code

Command	**local-auth qrcode ip** *ip-address*
Parameter Description	**ip**: Specifies the IP address for accessing the QR code. *ip-address*: Indicates the IP address.
Command Mode	Authentication server mode (config-app-auth-server). This command is available only when the server type is set to **qrcode-alone**.
Usage Guide	Use this command to configure the IP address for accessing the QR code.

Configuration Example

Configuring an IP Address for Accessing the QR Code

Configuration Steps	• Configure authentication server named qralone on the gateway, set the authentication mode to **qrcode-alone**, and set the IP address for accessing the QR code to 1.2.3.4.
	FS# configure terminal FS(config)# app-auth server qralone type qrcode-alone FS(config-app-auth-server)# local-auth act-directory source-ip 1.2.3.4
Verification	• Run the **show app-auth server all** command to display the authentication server configuration. FS# show app-auth server all server name: qralone type: qrcode-alone mode: alone comment: zizhu ip: 1.2.3.4 key: test

Common Errors

- N/A

21.4.27 Configuring a Dynamic Code for the QR Code

Configuration Effect

- Configure a dynamic code for the QR code. This dynamic code is used to check whether the QR code is valid.

Notes

- N/A

Configuration Steps

- Optional.

Verification

- Run the **show app-auth server all** command to display the configuration.

Related Commands

Configuring a Dynamic Code for the QR Code

Command	**local-auth qrcode key** *key-str*
Parameter Description	**key:** Specifies the dynamic code. *key-str*: Indicates the dynamic code string.
Command Mode	Authentication server mode (config-app-auth-server). This command is available only when the server type is set to **qrcode-alone**.
Usage Guide	Use this command to configure a dynamic code for the QR code.

Configuration Example

Configuring a Dynamic Code for the QR Code

Configuration Steps	• Configure authentication server named qralone on the gateway, and set the authentication mode to **qrcode-alone**, and the dynamic code to test.
	FS# configure terminal FS(config)# app-auth server qralone type qrcode-alone FS(config-app-auth-server)# local-auth qrcode key test
Verification	• Run the **show app-auth server all** command to display the authentication server configuration. FS# show app-auth server all server name: qralone type: qrcode-alone

	mode: alone comment: zizhu ip: 1.2.3.4 key: test

Common Errors

- N/A

21.4.28 Configuring a Comment on the QR Code

Configuration Effect

- Configure a comment on the QR code. This comment instructs visitors how to access the Internet.

Notes

- N/A

Configuration Steps

- Optional.

Verification

- Run the **show app-auth server all** command to display the configuration.

Related Commands

Configuring a Comment on the QR Code

Command	**local-auth qrcode comment** *comment-str*
Parameter Description	**comment**: Specifies the comment. *comment-str*: Indicates the comment string.
Command Mode	Authentication server mode (config-app-auth-server). This command is available only when the server type is set to **qrcode-alone** or **qrcode-authorize**.
Usage Guide	Use this command to configure a comment on the QR code.

Configuration Example

Configuring a Comment on the QR Code

Configuration Steps	• Configure authentication server named qralone, set the authentication mode to **qrcode-alone**, and set the comment to zizhu on the gateway.
	FS# configure terminal FS(config)# app-auth server qralone type qrcode-alone FS(config-app-auth-server)# local-auth qrcode comment zizhu

Verification	● Run the **show app-auth server all** command to display the authentication server configuration. FS# show app-auth server all server name: qralone type: qrcode-alone mode: alone comment: zizhu ip: 1.2.3.4 key: test

Common Errors

- N/A

21.4.29 Configuring Parameters Related to QR Code Authorization-based Authentication

Configuration Effect

- Configure parameters related to QR code authorization-based authentication.

Notes

- N/A

Configuration Steps

- Optional.

Verification

- Run the **show app-auth local-auth config** command to display the configuration.

Related Commands

Configuring Parameters Related to QR Code Authorization-based Authentication

Command	**app-auth local-auth** { **authorize** { **check** | **restrict-times** *times* } | **authorize-time** *minute* }
Parameter Description	**check**: Indicates whether the authorization function is enabled. **restrict-times**: Indicates the restricted number of times that an authorized user can grant the Internet access permission to other users. *time:* Specifies the number of times. **authorize-time**: Indicates the available Internet access duration of an authorized user. *minute*: Specifies the available Internet access duration after authorized authentication.
Command Mode	Global configuration mode

Usage Guide	N/A

Configuration Example

Configuring Parameters Related to QR Code Authorization-based Authentication

Configuration Steps	● Enable QR code authorization-based authentication on the gateway, and set the available Internet access duration after authentication to 60 minutes, and the number of times that an authorized user can grant the Internet access permission to other users to 3.
	FS# configure terminal FS(config)# app-auth local-auth authorize check FS(config)# app-auth local-auth authorize restrict-times 3 FS(config)# app-auth local-auth authorize-time 60

Verification	● Run the **show app-auth local-auth config** command to display the local authentication configuration.
	FS#show app-auth local-auth config
	enable: True
	data-store-enable: True
	data-store-age-day: 36
	user-mac-limit: 2
	online-time: 0
	authorize-time: 60
	restrict-range information:
	  mobile:
	  global: false
	  name:
	  state: Idle
	  pc:
	  global: false
	  name:
	  state: Idle

Common Errors

- N/A

21.4.30 Configuring Parameters of the SMS Server

Configuration Effect

- Configure parameters of the SMS server.

Notes

- N/A

Configuration Steps

- Optional.

Verification

- Run the **show app-auth server all** command to display the configuration.

Related Commands

Configuring Parameters of the SMS Server

Command	**local-auth sms keyid** *keyid-str* **keysecret** *keysecret-str* **sign** *sign-str* **templet** *templet-str*
Parameter Description	**Keyid**: Indicates appkey for SMS server-based authentication. *Keyid-str*: Specifies the specific appkey. **Keysecret**: Indicates secret-key for SMS-based authentication. *Keysecret-str*: Specifies the specific secret-key. **Sign**: Indicates the SMS signature. *Sign-str*: Specifies the SMS signature string. **Templet**: Indicates the SMS template. *Templet-str*: Specifies the SMS template string.
Command Mode	Authentication server mode (config-app-auth-server). This command is available only when the server type is set to **sms**.
Usage Guide	Use this command to configure parameters of the SMS server.

Configuration Example

Configuring Parameters of the SMS Server

Configuration Steps	● Configure authentication server named sms on the gateway and set the authentication mode to **sms**.
	FS# configure terminal FS(config)# app-auth server sms-auth type sms FS(config-app-auth-server)# local-auth sms keyid aaabbb keysecret cccddd sign eeefff templet ggghhh
Verification	● Run the **show app-auth server all** command to display the authentication server

	configuration. FS# show app-auth server all server name: sms-auth type: sms mode: 1 server: aliyun-v1 keyid: aaabbb keysecret: cccddd sign: eeefff templet: ggghhh

Common Errors

- N/A

21.4.31 Configuring the Type of the SMS Server

Configuration Effect

- Configure the type of the SMS server.

Notes

- N/A

Configuration Steps

- Optional.

Verification

- Run the **show app-auth server all** command to display the configuration.

Related Commands

Configuring the Type of the SMS Server

Command	**local-auth sms server** { **aliyun-v1** | **aliyun-v2** }
Parameter Description	**Server**: Indicates the type of the SMS server. **aliyun-v1**: Indicates Alibaba Cloud SMS v1. **aliyun-v2**: Indicates Alibaba Cloud SMS v2.
Command Mode	Authentication server mode (config-app-auth-server). This command is available only when the server type is set to **sms**.
Usage Guide	Use this command to configure the type of the SMS server.

Configuration Example

Configuring the Type of the SMS Server

Configuration Steps	● Configure authentication server named sms on the gateway, and set the authentication mode to **sms** and server type to Alibaba Cloud SMS v1.
	FS# configure terminal FS(config)# app-auth server sms-auth type sms FS(config-app-auth-server)# local-auth sms server aliyun-v1
Verification	● Run the **show app-auth server all** command to display the authentication server configuration. FS# show app-auth server all server name: sms-auth type: sms mode: 1 server: aliyun-v1 keyid: aaabbb keysecret: cccddd sign: eeefff templet: ggghhh

Common Errors

- N/A

21.4.32 Configuring the Mobile Phone Prior Mode in SMS-based Authentication

Configuration Effect

- Configure the mobile phone prior mode.

Notes

- N/A

Configuration Steps

- Optional.

Verification

- Run the **show app-auth server all** command to display the configuration.

Related Commands

Configuring the Prior Mode

Command	**local-auth sms mode prior**
Parameter Description	**mode**: Indicates the SMS mode. **prior**: Indicates the prior mode.
Command Mode	Authentication server mode (config-app-auth-server). This command is available only when the server type is set to **sms**.
Usage Guide	Use this command to configure the prior mode for SMS-based authentication.

Configuration Example

Configuring the Prior Mode

Configuration Steps	● Configure authentication server named sms on the gateway, and set the authentication mode to **sms** and mode to prior mode.
	FS# configure terminal FS(config)# app-auth server sms-auth type sms FS(config-app-auth-server)# local-auth sms mode prior
Verification	● Run the **show app-auth server all** command to display the authentication server configuration. FS# show app-auth server all server name: sms-auth type: sms mode: 1 server: aliyun-v1 keyid: aaabbb keysecret: cccddd sign: eeefff templet: ggghhh

Common Errors

- N/A

21.4.33 Configuring Parameters Related to WeChat-based Authentication

Configuration Effect

- Configure parameters related to WeChat-based authentication.

Notes

- N/A

Configuration Steps

- Optional.

Verification

- Run the **show app-auth server all** command to display the configuration.

Related Commands

Configuring Parameters Related to WeChat-based Authentication

Command	**local-auth weixin shopid** *shopid-str* **appid** *appid-str* **secretkey** *secretkey-str*
Parameter Description	**Shopid**: Indicates the shop ID. *Shopid*: Specifies the shop ID string. **appid**: Indicates the WeChat public platform account. *appid-str*: Specifies the appid string. secretkey: Indicates the signature key. *secretkey-str*: Specifies the secretkey string.
Command Mode	Authentication server mode (config-app-auth-server). This command is available only when the server type is set to **weixin**.
Usage Guide	Use this command to configure parameters related to WeChat-based authentication.

Configuration Example

Configuring Parameters Related to WeChat-based Authentication

Configuration Steps	• Configure authentication server named wechat on the gateway and set the authentication mode to **weixin**.
	FS# configure terminal FS(config)# app-auth server wechat type weixin FS(config-app-auth-server)# local-auth weixin shopid 111 appid bbb secretkey ccc
Verification	• Run the **show app-auth server all** command to display the authentication server configuration. FS# show app-auth server all server name: wechat type: weixin decrypt-flag: 0 shopid: 111 appid: bbb

	secretkey: ccc ssid: ssid_test

Common Errors

- N/A

21.4.34 Configuring the SSID of the Authentication Server

Configuration Effect

- Configure the SSID of the authentication server.

Notes

- N/A

Configuration Steps

- Optional.

Verification

- Run the **show app-auth policy** command to display the configuration.

Related Commands

Configuring the SSID of the Authentication Server

Command	**local-auth weixin ssid** *ssid-str*
Parameter Description	**ssid**: Indicates the SSID of the server. ***ssid-str***: Specifies the SSID string.
Command Mode	Authentication server mode (config-app-auth-server). This command is available only when the server type is set to **weixin**.
Usage Guide	Use this command to configure the SSID of the authentication server.

Configuration Example

Configuring the SSID of the Authentication Server

Configuration Steps	- Configure authentication server named wechat on the gateway, and set the type to **weixin** and SSID to ssid_test.
	FS# configure terminal FS(config)# app-auth server wechat type weixin FS(config-app-auth-server)# local-auth weixin ssid ssid_test
Verification	- Run the **show app-auth server all** command to display the authentication server

	configuration. FS# show app-auth server all server name: wechat type: weixin decrypt-flag: 0 shopid: 111 appid: bbb secretkey: ccc ssid: ssid_test

Common Errors

- N/A

21.4.35 Configuring an Authentication Policy Group

Configuration Effect

- Configure an authentication policy group.

Notes

- N/A

Configuration Steps

- Optional.

Verification

- Run the **show app-auth policy all** command to display the configuration.

Related Commands

Configuring an Authentication Policy Group

Command	**app-auth policy** *name*
Parameter Description	**policy**: Indicates an authentication policy. *name*: Specifies the policy name.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure an authentication policy group.

Configuration Example

Configuring an Authentication Policy Group

Configuration Steps	● Configure authentication policy named aaa on the gateway.
	FS# configure terminal FS(config)# app-auth policy aaa
Verification	● Run the **show app-auth policy** command to display the authentication policy. FS#show app-auth policy all Global information: policy_cnt : 1 Global Ip-range 001. 0.0.0.0 ~ 255.255.255.255 Detail: Policy aaa enable: True pid: 2 mode: pwd state: 0 ip-range number: 1 cfile-path: plcy2.php sms: 1 weixin: 1 ip-range info: 1. ALL server number 2: 1. name:adf type: sms 2. name:wechat type: weixin

Common Errors

- N/A

21.4.36 Enabling Authentication Policy

Configuration Effect

- Enable authentication policy.

Notes

- N/A

Configuration Steps

- Optional.

Verification

- Run the **show app-auth policy all** command to display the configuration.

Related Commands

Enabling an Authentication Policy

Command	**rule enable**
Parameter Description	**enable**: Enables this policy.
Command Mode	APP-AUTH policy group configuration mode
Usage Guide	Use this command to enable an authentication policy. This command is available only in APP-AUTH policy group mode.

Configuration Example

Enabling an Authentication Policy

Configuration Steps	- Configure authentication policy named abc on the gateway and make it effective.
	FS# configure terminal FS(config)# app-auth policy aaa FS(app-auth-policy)# rule enable
Verification	- Run the **show app-auth policy all** command to display the authentication policy. FS#show app-auth policy all Global information: policy_cnt : 1 Global Ip-range 001. 0.0.0.0 ~ 255.255.255.255 Detail: Policy aaa enable: True

```
  pid: 2
  mode: pwd
  state: 0
  ip-range number: 1
  cfile-path: plcy2.php
  sms: 1
  weixin: 1
ip-range info:
    1. ALL
  server number 2:
    1. name:adf      type: sms
    2. name:wechat      type: weixin
```

Common Errors

- This command is available only in APP-AUTH policy group mode.

21.4.37 Configuring an IP Address Range in Which an Authentication Policy Is Effective

Configuration Effect

- Configure an IP address range in which an authentication policy is effective.

Notes

- N/A

Configuration Steps

- Optional.

Verification

- Run the **show app-auth policy all** command to display the configuration.

Related Commands

↘ Configuring an IP Address Range in Which an Authentication Policy Is Effective

Command	**rule ip-range** { [*ip1* { *ip2* }] | **all** }
Parameter Description	*ip1*: Indicates the start IP address. *ip2*: Indicates the end IP address. **all**: Indicates that the authentication policy takes effect on all IP addresses.
Command Mode	APP-AUTH policy group configuration mode
Usage Guide	Use this command to configure an IP address range in which an authentication policy is

	effective. This command is available only in APP-AUTH policy group mode.

Configuration Example

Configuring an IP Address Range in Which an Authentication Policy Is Effective

Configuration Steps	● Configure authentication policy named aaa on the gateway and make it effective on all IP addresses.
	FS# configure terminal FS(config)# app-auth policy aaa FS(app-auth-policy)# rule ip-range all
Verification	● Run the **show app-auth policy all** command to display the authentication policy.

```
FS#show app-auth policy all
Global information:
policy_cnt : 1
Global Ip-range
001. 0.0.0.0 ~ 255.255.255.255


Detail:
Policy aaa
   enable: True
   pid: 2
   mode: pwd
   state: 0
   ip-range number: 1
   cfile-path: plcy2.php
   sms: 1
   weixin: 1
ip-range info:
      1. ALL
   server number 2:
      1. name:adf       type: sms
      2. name:wechat       type: weixin
```

Common Errors

- This command is available only in APP-AUTH policy group mode.

21.4.38 Configuring an Authentication Server Associated with an Authentication Policy

Configuration Effect

- Configure an authentication server associated with an authentication policy.

Notes

- N/A

Configuration Steps

- Optional.

Verification

- Run the **show app-auth policy all** command to display the configuration.

Related Commands

Configuring an Authentication Server Associated with an Authentication Policy

Command	**relate server** *server-name*
Parameter Description	**server**: Indicates the associated authentication server. *server-name*: Specifies the name of the authentication server.
Command Mode	APP-AUTH policy group configuration mode
Usage Guide	This command is available only in APP-AUTH policy group mode.

Configuration Example

Configuring an Authentication Server Associated with an Authentication Policy

Configuration Steps	• Configure authentication policy named aaa on the gateway and associate it with authentication server named wechat.
	FS# configure terminal FS(config)# app-auth policy aaa FS(app-auth-policy)# relate server wechat
Verification	• Run the **show app-auth policy all** command to display the authentication policy. FS#show app-auth policy all Global information: policy_cnt : 1

```
Global Ip-range
001. 0.0.0.0 ~ 255.255.255.255


Detail:
Policy aaa
  enable: True
  pid: 2
  mode: pwd
  state: 0
  ip-range number: 1
  cfile-path: plcy2.php
  sms: 1
  weixin: 1
ip-range info:
    1. ALL
  server number 1:
    1. name:wechat      type: weixin
```

Common Errors

- This command is available only in APP-AUTH policy group mode.

21.4.39 Configuring the Authentication Type of an Authentication Policy

Configuration Effect

- Configure the authentication type of an authentication policy.

Notes

- N/A

Configuration Steps

- Optional.

Verification

- Run the **show app-auth policy all** command to display the configuration.

Related Commands

Configuring the Authentication Type of an Authentication Policy

Command	**rule type pwd**
Parameter Description	**pwd**: Indicates the account- and password-based authentication.
Command Mode	APP-AUTH policy group configuration mode
Usage Guide	This command is available only in APP-AUTH policy group mode.

Configuration Example

Configuring the Authentication Type of an Authentication Policy

Configuration Steps	● Configure authentication policy named aaa on the gateway and configure account- and password-based authentication.
	FS# configure terminal FS(config)# app-auth policy aaa FS(app-auth-policy)# rule type pwd
Verification	● Run the **show app-auth policy all** command to display the authentication policy. FS#show app-auth policy all Global information: policy_cnt : 1 Global Ip-range 001. 0.0.0.0 ~ 255.255.255.255 Detail: Policy aaa enable: True pid: 2 mode: pwd state: 0 ip-range number: 1 cfile-path: plcy2.php sms: 1 weixin: 1 ip-range info: 1. ALL

	server number 1: 1. name:wechat type: weixin

Common Errors

- This command is available only in APP-AUTH policy group mode.

21.4.40 Configuring the Available Online Duration for Local Users Who Are Successfully Authenticated

Configuration Effect

- After successful authentication, unauthorized users can access the Internet for this period of time.

Notes

- N/A

Configuration Steps

- Optional.

Verification

- Run the **show app-auth local-auth config** command to display the configuration.

Related Commands

↘ Configuring the Available Online Duration for Local Users Who Are Successfully Authenticated

Command	**app-auth local-auth online-time** *time*
Parameter Description	**online-time**: Indicates the available online duration of local users who are successfully authenticated. *time*: Specifies the duration, in minutes.
Command Mode	Global configuration mode
Usage Guide	This command is unavailable to authorized users passing authentication.

Configuration Example

↘ Configuring the Available Online Duration for Local Users Who Are Successfully Authenticated

Configuration Steps	● Set the available online duration to 10 minutes for local users who are successfully authenticated on the gateway.
	FS# configure terminal FS(config)# app-auth local-auth online-time 10
Verification	● Run the **show app-auth local-auth config** command to display the local authentication

	configuration. FS# show app-auth local-auth config enable: True data-store-enable: True data-store-age-day: 36 user-mac-limit: 2 online-time: 10 authorize-time: 33 restrict-range information: mobile: global: false name: state: Idle pc: global: false name: state: Idle

Common Errors

- This command is unavailable to authorized users passing authentication.

21.4.41 Restricting Clients in Specific Types from Internet Access

Configuration Effect

- Restrict clients in specific types from Internet access.

Notes

- N/A

Configuration Steps

- Optional.

Verification

- Run the **show app-auth local-auth config** command to display the configuration.

Related Commands

↘ **Restricting Clients in Specific Types from Internet Access**

Command	**app-auth local-auth restrict** { **pc** | **mobile** } [**exclude time-range** *time*]
Parameter Description	**pc**: Restricts PCs from Internet access. **mobile**: Restricts mobile phones from Internet access. *time*: Indicates the start time, from which the Internet access is not restricted.
Command Mode	Global configuration mode
Usage Guide	Use this command to restrict the Internet access behaviors of users.

Configuration Example

Restricting Clients in Specific Types from Internet Access

Configuration Steps	● Restrict mobile users from Internet access except in the "day" time period.
	FS# configure terminal FS(config)# app-auth local-auth restrict mobile exclude time-range day

Verification	● Run the **show app-auth local-auth config** command to display the local authentication configuration.
	FS# show app-auth local-auth config
	enable: True
	data-store-enable: True
	data-store-age-day: 36
	user-mac-limit: 2
	online-time: 1
	authorize-time: 33
	restrict-range information:
	  mobile:
	  global: true
	  name: day
	  state: Not exist
	  pc:
	  global: false
	  name:
	  state: Idle

21.5 Monitoring

Displaying

Description	Command
Displays online clients.	**show app-auth online**
Displays all client information.	**show app-auth user all**
Displays parameter configuration related to APP-AUTH.	**show app-auth statistics**
Displays network segment configuration.	**show app-auth auth-rule**
Displays APP-AUTH configuration.	**show app-auth cfg-opt**
Displays an authentication-free IP address range.	**show app-auth direct-srcip**
Displays an authentication-free extranet resource range.	**show app-auth direct-dstip**
Displays a MAC address whitelist.	**show app-auth direct-mac**
Displays a MAC address blacklist.	**show app-auth deny-mac**
Displays network segment configuration rules.	**show app-auth auth-rule**
Displays network segment and SSID configuration.	**show app-auth ssid-cfg**
Displays TCP keepalive connection configuration.	**show app-auth tcp-info**
Displays the HTTPS re-direction information.	**show app-auth proxy-option config**
Displays the local authentication configuration.	**show app-auth local-auth config**
Displays information about the authentication policy.	**show app-auth policy**
Displays information about VIP users.	**show app-auth local-auth vip-group**
Displays information about locally authenticated users.	**show app-auth local-auth subs**
Displays information about online users who are locally authenticated.	**show app-auth local-online**

22 Configuring Webservice

22.1 Overview

Webservice is used to coordinate with APP-AUTH to control HTTP interaction with the server.

Webservice is similar to the Web service, and the specific service logic of Webservice is controlled by APP-AUTH.

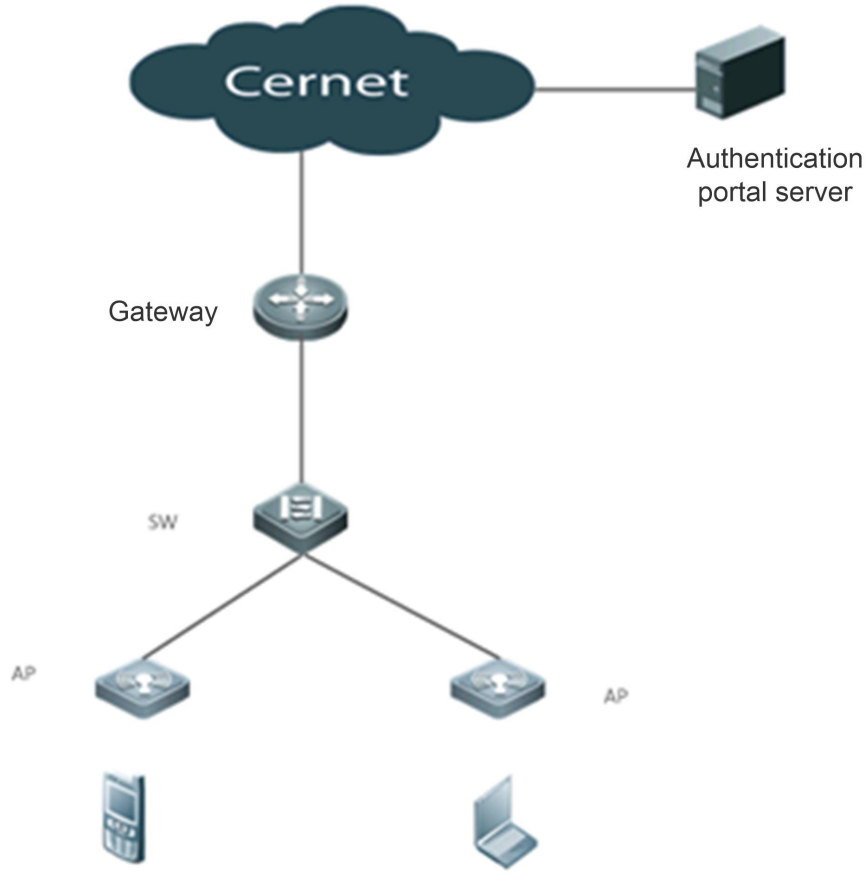
22.2 Applications

Application	Description
Applying Webservice	Describes the typical application of Webservice.

22.2.1 Applying Webservice

Scenario

As shown in the following figure, a mobile client is successfully authenticated by an authentication server and accesses a network via a gateway.



Remarks	The authentication server can be a FS WMC or MCP, or a third-party server that complies with an authentication protocol of APP-AUTH.

Webservice provides the HTTP server and HTTP client functions, to implement HTTP interaction between the gateway and authentication server.

22.3 Features

Working Principle

Webservice can act as an HTTP server to receive HTTP requests from clients. For example, after the clients pass APP-AUTH authentication in WiFiDog mode, the token verification requests initiated by the clients are received by Webservice. Webservice can also act as an HTTP client to initiate token verification to the server.

22.4 Configuration

Configuration	Description and Command	
Configuring Server IP Address	(Optional) It is used to configure server IP addresses. When WiFi connection over WeChat is selected, WiFiDog must be supported as well.	
	webservice service-url *url*	Configures Server IP Address 1.
	webservice sec-service-url *url*	Configures Server IP Address 2.
Configuring Server Detection	(Optional) It is used to detect whether the server is normal.	
	webservice portal-check [**enable** | **interval** *time_1* | **retransmit** *num*]	Detects the server status.
Configuring Monitoring Server Type	(Optional) It is used to configure a monitoring server.	
	webservice monitor fmt *xwc*	Configures the monitoring server type.

22.4.1 Configuring Server IP Address

Configuration Effect

- Enable the gateway to communicate with the server according to protocol stipulations.

Notes

- A server IP address is configured according to the selected protocol.

Configuration Steps

- Optional.
- If either WiFi connection over WeChat or WiFiDog is sufficient, run the **webservice service-url** command. If both WiFi connection over WeChat and WiFiDog are needed, run the **webservice service-url** command to configure the server address supporting WiFi connection over WeChat and run the **webservice sec-service-url** command to configure the server address supporting WiFiDog.

Verification

- Run the **show webservice config** command to display the configuration result.

Related Commands

Configuring Server IP Address 1

Command	**webservice service-url** *url*
Parameter Description	*url*: Indicates the server IP address.
Command Mode	Global configuration mode
Usage Guide	Use this command to set the server IP address to support WiFi connection over WeChat or WiFiDog.

Configuring Server IP Address 2

Command	**webservice sec-service-url** *url*
Parameter Description	*url*: Indicates the server IP address.
Command Mode	Global configuration mode
Usage Guide	Use this command to enable both WiFi connection over WeChat and WiFiDog. Server IP Address 1 is set to support WiFi connection over WeChat and Server IP Address 2 is set to support WiFiDog.

Configuration Example

Configuring WiFi Connection over WeChat and WiFiDog

Configuration Steps	Configure WiFi connection over WeChat in APP-AUTH. In Webservice, set Server IP Address 1 to support WiFi connection over WeChat and Server IP Address 2 to support WiFiDog.
	FS# configure terminal FS(config)# app-auth enable FS(config)# app-auth cwmp enable FS(config)# app-auth cfg-opt rdt-for-wx2 FS(config)# app-auth ad-url http://wmc.fsyun.com/auth/servlet/standardAuthServlet/portal FS(config)# webservice service-url http://wmc.fsyun.com/auth/servlet/standardAuthServlet/portal FS(config)# webservice sec-service-url http://wmc.fsyun.com/auth/wifidogAuth
Verification	Run the **show app-auth statistic** and **show webservice** commands separately to display the configuration result.

22.4.2 Configuring Server Detection

Configuration Effect

- Ensure that all clients do not need authentication if the server is abnormal.

Notes

- This function is enabled only after it is confirmed that the server supports this function. Otherwise, all clients do not need authentication.

Configuration Steps

- Optional.

Verification

- Run the **show webservice config** command to display the configuration result.

Related Commands

Configuring Server Detection

Command	**webservice portal-check** [**enable** | **interval** *time_1* | **retransmit** *num*]
Parameter Description	**enable**: Enables server detection. *time_1*: Specifies the detection interval. *num*: Indicates the number of retrial times.
Command Mode	Global configuration mode
Usage Guide	Use this command to cancel client authentication if the server is abnormal.

22.4.3 Configuring Monitoring Server Type

Configuration Effect

- Advertise client information to the monitoring server after the client is successfully authenticated.

Notes

- This function is enabled only after it is confirmed that the server supports this function.

Configuration Steps

- Optional.

Verification

- Run the **show run | i monitor fmt** command to display the configuration result.

Related Commands

Configuring Monitoring Server Type

Command	**webservice monitor fmt** *xwc*
Parameter Description	*xwc*: Indicates a Pronetway monitoring server.
Command Mode	Global configuration mode
Usage Guide	Use this command to advertise client information to the monitoring server after the client is successfully authenticated.

22.5 Monitoring

Displaying

Description	Command
Displays configuration related to Webservice.	**show webservice config**

23 Configuring ANTI-PAP

23.1 Overview

Anti personal access point (ANTI-PAP) can detect the user behavior of using a personal access point (AP) for network access. When such behavior is detected, the user will be prohibited from accessing external networks for a certain period.

ANTI-PAP can prevent uncontrollable access devices on the network, thereby ensuring network security to a certain extent. In addition, it can prevent personal APs from affecting wireless signals of valid APs.

23.2 Applications

Application	Description
Preventing Intranet Users from Using Personal APs	Intranet clients access the Internet directly via valid APs and cannot access the Internet via personal APs.

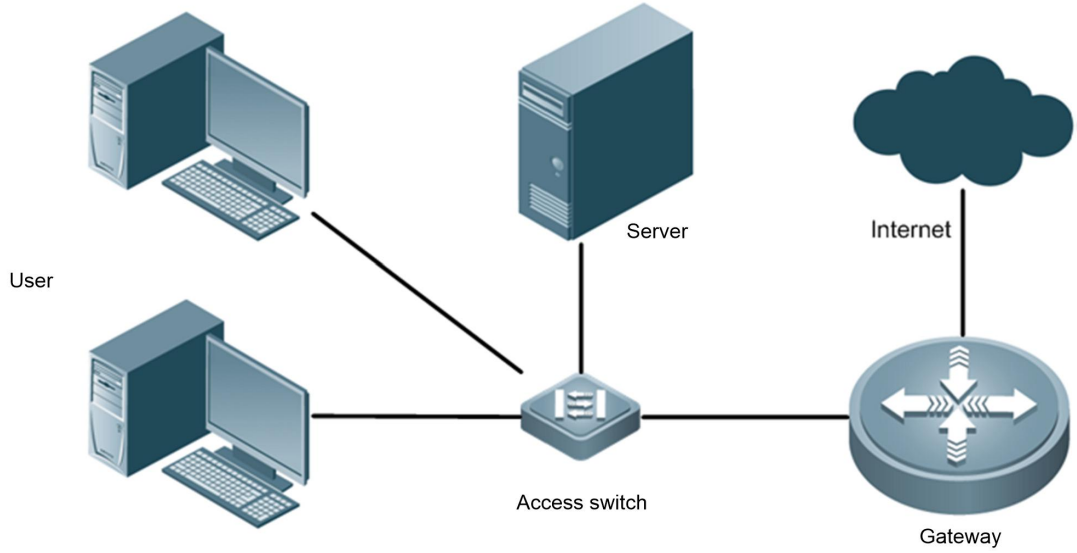
23.2.1 Preventing Intranet Users from Using Personal APs

Scenario

Intranet clients access the Internet directly via valid APs and cannot access the Internet via personal APs.

- On the intranet, clients that share the same IP address are not allowed to access the Internet.

Figure 23-1



Deployment

- Configure the user group to be detected and the blocking mode on the device to detect and block the unauthorized connection to personal APs.

23.3 Features

Overview

Feature	Description
Detecting Personal APs	Checks whether a user uses a personal AP for network access.

23.3.1 Detecting Personal AP

The device detects the network traffic of a user. Once it discovers a personal AP, it restricts network access of the user by blocking access or limiting the rate.

Working Principle

A personal AP always connects to multiple clients. Therefore, personal AP detection is essentially client quantity detection.

User agent detection and virtual identity quantity detection are methods available for client detection.

User Agent Detection

User agent, UA for short, is a field in the header of an HTTP request packet. The field contains content such as the operating system and version, CPU type, browser and version, browser rendering engine, browser language, and browser plug-in of the client, which can be used to identify the client.

Virtual Identity Quantity Detection

The virtual identity audit function of the content audit module can audit the go-online and go-offline actions of a virtual identify. For some common applications such as WeChat and Taobao, this function can determine whether there are multiple clients based on the number of concurrent online accounts.

23.4 Configuration

Configuration	Description and Command	
Configuring Users to Be Detected	(Mandatory) It is used to designate a user to be detected.	
	anti-pap monitor	Configures a user to be detected.
Configuring Blocking-free Server Resources	(Optional) It is used to prevent access to special servers from being blocked by the device, for example, access to the authentication server.	
	anti-pap avoid-block	Adds a blocking-free server resource.

23.4.1 Configuring Users to Be Detected

Configuration Effect

- Detect Internet access behaviors of a designated user to determine whether there is a personal AP.

Notes

- This function relies on the processing results of application identification, flow audit, and virtual identity audit. Therefore, these three functions can be enabled to enhance the detection effect.

Configuration Steps

Configuring Users to Be Detected

- Mandatory.

Command	**anti-pap monitor** { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } } [**expected-terminal** { **pc** | **mobile** }] [{ **block** [*time*] | **limit** *down up* } **base** { **user** | **ip** }]
Parameter Description	**subscriber** *subs-name1*: Specifies the local username to be detected. **Subscriber any**: Specifies that all local users will be detected. **auth-subscriber** *subs-name2*: Specifies the authenticated username to be detected. **auth-aubscriber any**: Specifies that all authenticated users will be detected. **expected-terminal { pc | mobile }**: Specifies the expected client type. The default type is any type. **block**: Specifies whether blocking is enabled. Blocking is disabled by default. *time*: Indicates the blocking period in minutes. The value range is from **1** to **1440**. The default value is **10**. **limit**: Indicates the user bandwidth limit. The rate is not limited by default. *down*: Indicates the downlink bandwidth. *up*: Indicates the uplink bandwidth. **user**: Indicates blocking by username. **ip**: Indicates blocking by IP address.
Defaults	No user is detected by default.
Command Mode	Global configuration mode
Usage Guide	Generally, the username is set to a user group name. Rules of authenticated users have higher priorities than those of local users, and rules of lower-level users have higher priorities than those of upper-level users.

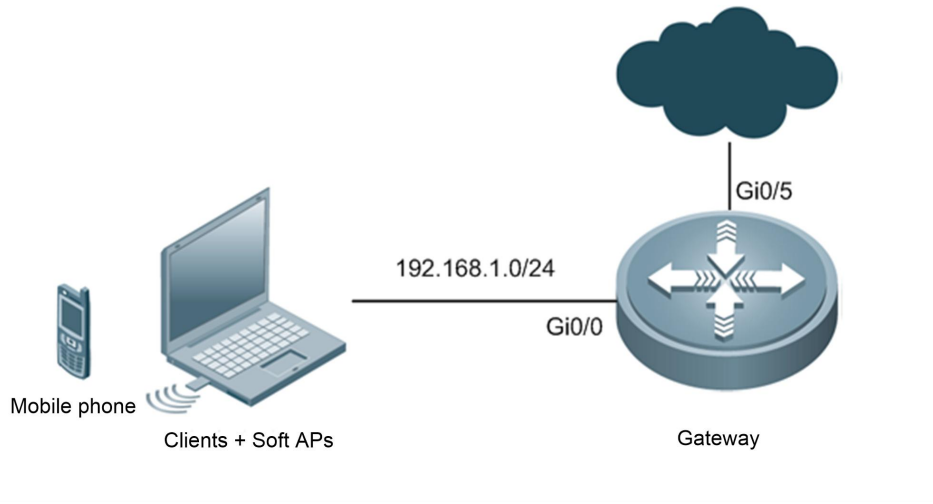
Verification

Verify that a user uses a personal AP and multiple clients to access the Internet.

- Verify that the user's access to the Internet is blocked.

Configuration Example

Detecting Users Within the Address Range 192.168.1.2–192.168.1.254

Scenario Figure 23-2	
Configuration Steps	● Define a user group and users. ● Configure the users as users to be detected.
	FS# configure terminal FS(config)# subscriber static name "19#students" parent "/" ip-range 192.168.0.2 192.168.0.254 FS(config)# anti-pap monitor 19#students FS(config)# end
Verification	
	A user uses a wireless network interface card (NIC) as a soft AP to provide the wireless network service for mobile phones, and uses two clients to access the Internet at the same time. ● Internet access of the user is blocked.

23.4.2 Configuring Blocking-free Server Resources

Configuration Effect

- Allow blocked users to access designated servers.

Notes

- The function is configured only when packets of the users for accessing these servers pass through the device.

Configuration Steps

Configuring Blocking-free Server Resources

- Optional.

Command	**anti-pap avoid-block ip-group** *id*
Parameter Description	*id*: Indicates the ID of the IP object group.
Defaults	No blocking-free server is configured by default.

Command Mode	Global configuration mode
Usage Guide	A server resource must be defined by running the **ip-group** command before it can be referenced by this command.

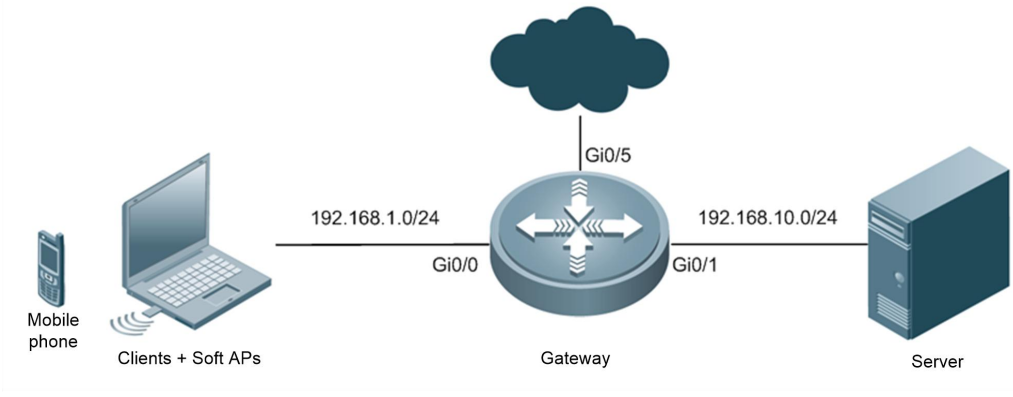
Verification

Verify that traffic of a user that uses a personal AP and multiple clients to access network is blocked, or the traffic of the user is directly and manually blocked.

- Verify that access of the user to blocking-free servers is not affected, but other traffic that passes through the device is blocked.

Configuration Example

Adding Address Range 192.168.10.2–192.168.10.254 to Blocking-free Server Resources

Scenario Figure 23-3	
Configuration Steps	- Define the IP object group of blocking-free servers. - Add the IP object group to the blocking-free server resources.
	FS# configure terminal FS(config)# ip-group 3 FS(config-ip-group)# ip-range 192.168.10.2 192.168.10.254 FS(config-ip-group)# exit FS(config)# anti-pap avoid-block ip-group 3 FS(config)# end
Verification	
	A user uses a wireless NIC as the soft AP to provide the wireless network service for mobile phones, and uses two clients to access the Internet at the same time. As a result, access of the user is blocked, or is directly and manually blocked. - The user can access the blocking-free servers but cannot access the Internet.

23.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears the limit on the designated users.	**clear anti-pap control** { { { **subscriber** *subs-name1* | **auth-subscriber** *subs-name2* } } | **ip** *addr* }

Displaying

Description	Command
Displays the configuration information.	**show anti-pap config**
Displays logs.	**show anti-pap log from** *y1 m1 d1* [*H1:M1:S1*] **to** *y2 m2 d2* [*H2:M2:S2*] [**subscriber** *subs-name1* | **auth-subscriber** *subs-name2*] [**ip** *addr*] **order-by** { **time** | **subscriber** | **auth-subscriber** | **ip** } { **asc** | **desc** } [**start-item** *num1* **end-item** *num2*]
Displays the user detection information.	**show anti-pap user** [**subscriber** *subs-name1* | **auth-subscriber** *subs-name2*] [**ip** *addr*]

24 Configuring WEB-ADVERT

24.1 Overview

Advertisement push is a method of enabling a Network Access Device (NAS) to force the browser to display a specific advertisement window when users access the Internet via the browser. It is a sub function of Web authentication. The principle of advertisement push is described as follows: On the basis of the Hypertext Transfer Protocol (HTTP) interception and HTTP redirection technologies of FS Web authentication, the NAS first intercepts an HTTP or Hypertext Transfer Protocol Secure (HTTPS) packet of an advertisement user (other packets are not intercepted), conducts redirection (redirects the browser to the configured advertisement address), and then releases the HTTP/HTTPS packet of the user.

Protocols and Standards

- HTTP: RFC1945 RFC2068
- HTTPS: RFC2818

24.2 Applications

Application	Description
Applying Advertisement Push in Basic Scenarios	In the common basic scenario of Layer-2 advertisement push, the NAS pushes advertisements and users are connected to the NAS via the Layer-2 network.

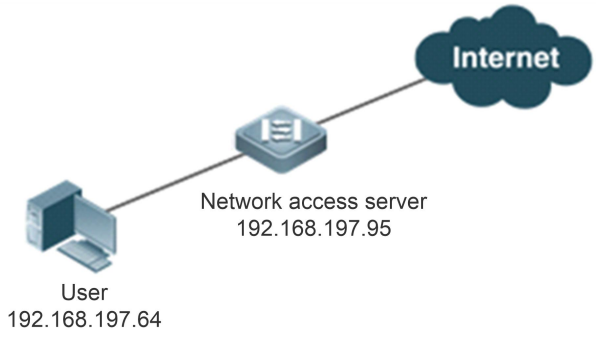
24.2.1 Applying Advertisement Push in Basic Scenarios

Scenario

As shown in Figure 17-1 The client connected to the NAS needs to pass Web authentication before accessing the Internet.

- Deploy the advertisement push scheme on the NAS.
- The user connected to the NAS can access the Internet only after the specified advertisement is pushed to the user.

Figure 24- 1 Network Topology of Advertisement Push Scheme



Deployment

- Enable advertisement push globally on the NAS.
- Configure the network segment range of advertisement push on the NAS.

24.3 Features

Basic Concepts

➘ Advertisement Push Scheme

Users are connected to the NAS via a Layer-2 network. The NAS intercepts HTTP/HTTPS packets (other packets are not intercepted) from the advertisement users, conducts redirection (redirects their browsers to the configured advertisement address), and then releases the HTTP/HTTPS packets of the users.

➘ HTTP Interception

HTTP interception refers that the NAS intercepts the HTTP packets to be forwarded. These HTTP packets are transmitted by the browsers of the users connected to the NAS but they are not destined for the NAS. For example, a user accesses www.google.com via the Internet Explorer (IE). The NAS is supposed to forward HTTP requests from the user to the gateway. If HTTP interception is enabled, these packets will not be forwarded.

After HTTP interception is enabled, the NAS diverts HTTP connection requests of a user to the NAS itself. Then, a connection session is established between the NAS and the user. The HTTP redirection function enables the NAS to push a redirection page to the user. Then, a page will be displayed on the browser of the user. The page can be an authentication page or a page that provides the link for downloading software.

You can specify the users whose HTTP packets destined for destination ports (Port 80 and Port 443 currently) need (or do not need) to be intercepted in the advertisement function. In general, HTTP requests from users, to whom no advertisement is pushed, will be intercepted and HTTP requests from users, to whom advertisements have been pushed, will not be intercepted. HTTP interception is the basis of the advertisement function. The interception of an HTTP packet transmitted by a browser automatically triggers the advertisement push process.

➘ HTTP Redirection

According to the HTTP protocol, in normal cases, after a user browser sends the HTTP GET or HEAD request, if the application to which the user initiates a HTTP request can provide resources, it responds with the 200 response; if the application cannot provide resources, it responds with the 302 response. In the 302 response, a new site path is provided. After receiving the response, the user can sends the HTTP GET or HEAD packet to the new site to request resources. This is called redirection.

HTTP redirection is an important part of the advertisement push function. It takes effect after HTTP interception is enabled and utilizes the feature of the HTTP 302 response. A connection session is established between the NAS and a user during HTTP interception. Afterwards, the user sends the HTTP GET or HEAD packet (that is supposed to be sent to another site) to the NAS. After receiving the packet, the NAS responds with the 302 response and adds the site path of the redirection page to the 302 response. In this way, the user resends a request to the site path to access the redirected page.

Overview

Feature	Description
Advertisement Push	Pushes advertisements to users via the NAS.

24.3.1 Advertisement Push

Working Principle

Roles of advertisement push:

1 Client: Usually refers to the browser running HTTP. When a user accesses the Internet via a browser, the browser will send HTTP requests.
2 NAS: Generally refers to an access-layer device in the network topology. It is directly connected to user terminals and the advertisement push function needs to be enabled on the NAS.

Advertisement push process:

1. The NAS intercepts an HTTP/HTTPS packet transmitted by an advertisement user and forwards the packet to a specific port listened by the Web authentication component via the inpath component.
2. After the Web authentication component receives the packet, if the advertisement push function is enabled and the network address of the user is within the network segment range of advertisement push, the Web authentication component forwards the packet to the advertisement sub module. The advertisement sub module transmits a redirection response to redirect the browser from the address to be accessed by the user to the advertisement address. Then, an advertisement page is displayed on the browser of the user.
3. After redirection is completed, the advertisement sub module records user information, configures an access user entry through the SCC interface, and releases the HTTP/HTTPS packet of the user.

User go-offline:

1 Case 1: The advertisement function is disabled. After the **no advertising enable** command is executed to disable the advertisement function, the NAS deletes information about all advertisement users and forces the users to go offline.
2 Case 2: The configuration of the network segment, to which an advertisement is pushed, is deleted. The NAS deletes information about advertisement users in the network segment and forces the users to go offline.
3 Case 3: If the periodical interception function is enabled, when the interval timer expires, the advertisement sub module finds out user information that timed out, deletes entries of these access users through the SCC interface, and pushes advertisements to the users when they send HTTP/HTTPS packets later.

Related Configuration

Configuring URL of Advertisement Pop-up Box

By default, no URL is configured for an advertisement pop-up box.

Run the **advertising url** { *url-string* } command in global configuration mode to configure the URL of an advertisement pop-up box.

Configuring Network Segment Range for Advertisement Push

By default, no network segment range is configured for advertisement push.

Run the **advertising free-user ip** { *ip-address* } **mask** { *ip-mask* } command in global configuration mode to configure a network segment range for advertisement push.

Enabling Advertisement Function

By default, the advertisement function is disabled.

Run the **advertising enable** command in global configuration mode to enable the advertisement function.

Enabling Periodical Interception

By default, periodical interception is disabled.

Run the **advertising suppress** command in global configuration mode to enable periodical interception.

Configuring Periodical Interception Interval

By default, the periodical interception interval is not configured.

Run the **advertising min-interval** { *interval-value* } command in global configuration mode to configure the periodical interception interval.

Enabling Function of Preventing Advertisement Pop-up Boxes from Being Intercepted by Browser

By default, the function of preventing advertisement pop-up boxes from being intercepted by the browser is disabled.

Run the **advertising popup-page** command in global configuration mode to enable the function of preventing advertisement pop-up boxes from being intercepted by the browser.

24.4 Configuration

Configuration	Description and Command	
Configuring Advertisement Push	(Mandatory) It is used to configure basic parameters for the advertisement function.	
	advertising url	Configures the URL of an advertisement pop-up box.
	advertising free-user ip mask	Configures a network segment range for advertisement push.
	advertising enable	Enables the advertisement function globally.
	(Optional) It is used to configure auxiliary parameters for the advertisement function.	
	advertising suppress	Enables periodical interception.
	advertising popup-page	Enables the function of preventing advertisement pop-up boxes from being intercepted by the browser.
	advertising min-interval	Configures the periodical interception interval.

24.4.1 Configuring Advertisement Push

Configuration Effect

An advertisement window pops up on the user browser.

Configuration Steps

Configuring URL of Advertisement Pop-up Box

- Mandatory. The URL of an advertisement pop-up box must be configured so that the advertisement push function is applied successfully.

Configuring Network Segment Range for Advertisement Push

- Mandatory. The network segment range of advertisement push must be configured so that the advertisement push function is applied successfully.
- When identifying that an unauthenticated user is accessing network resources, the NAS checks whether to push advertisements to the user according to the network segment range of advertisement push and the advertisement function.
- A maximum of 50 network segments can be configured.

Enabling Advertisement Function Globally

- Mandatory.
- By default, the advertisement function is disabled, and no advertisement is pushed to any connected user.

Enabling Periodical Interception

- Optional.
- By default, periodical interception is disabled, and advertisements are pushed to all connected users only once.

Configuring Periodical Interception Interval

- Optional.
- When periodical interception is disabled, the default value is 0.
- When periodical interception is enabled, the default value is 30.
- After periodical interception is enabled, the NAS periodically pushes advertisements to connected users at the configured interval.

Enabling Function of Preventing Advertisement Pop-up Boxes from Being Intercepted by Browser

- Optional.
- By default, the function of preventing advertisement pop-up boxes from being intercepted by the browser is disabled.

Verification

- If the attributes (for example, IP address) of a new user conforms to advertisement push rules, the NAS pushes advertisements to the user and then forces the user go online.
- After the user goes online, the user can access the Internet normally and the NAS no longer pushes advertisements to the user.

Related Commands

Configuring URL of an Advertisement Pop-up Box

Command	**advertising url** { *url-string* }
Parameter Description	*url-string*: Indicates the URL of an advertisement pop-up box.
Command Mode	Global configuration mode
Usage Guide	The URL begins with http:// or https://.

Configuring Network Segment Range for Advertisement Push

Command	**advertising free-user ip** { *ip-address* } **mask** { *ip-mask* }
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	A maximum of 50 network segments can be configured.

Enabling Advertisement Function Globally

Command	**advertising enable**

Parameter Description	*N/A*
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling Periodical Interception

Command	**advertising suppress**
Parameter Description	*N/A*
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Periodical Interception Interval

Command	**advertising min-interval** { *interval-value* }
Parameter Description	*N/A*
Command Mode	Global configuration mode
Usage Guide	The allowed interval ranges from 30 to 1440.

Enabling Function of Preventing Advertisement Pop-up Boxes from Being Intercepted by Browser

Command	**advertising popup-page**
Parameter Description	*N/A*
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Scenario	N/A
Configuration Steps	● Enable the advertisement function in global configuration mode on the NAS.
	FS# config Enter configuration commands, one per line. End with CNTL/Z. FS(config)# advertising url http://www.baidu.com/ FS(config)# advertising free-user ip 192.168.197.0 mask 255.255.255.0
	FS(config)# advertising enable
	FS(config)# advertising suppress FS(config)# advertising min-interval 40 FS(config)# advertising popup-page

Verification	● Check whether advertisement push is configured successfully.
	FS#show running-config … advertising popup-page advertising enable advertising free-user ip 192.168.197.0 mask 255.255.255.0 advertising min-interval 40 advertising url http://www.baidu.com/ advertising suppress ….
	FS#show advertising advertising enable: On advertising url: http://www.baidu.com/ advertising suppress: On advertising popup-page: On advertising min-interval: 40 advertising free-user: 192.168.197.0 255.255.255.0

24.5 Monitoring

Clearing

Description	Command
Forces an online user to go offline.	**clear web-auth user** { **all** | **ip** *ip-address* | **mac** *mac-address* | **name** *name-string* | **session-id** *num* }

Displaying

Description	Command
Displays basic parameters of the advertisement function.	**show advertising**
Displays the network segment range of advertisement push.	**show advertising free-user**
Displays all advertisement users.	**show advertising user**
Displays information about all online users or a specified online user.	**show web-auth user**{ **all** | **ip** *ip-address* | **mac** *mac-address* | **name** *name-string* | **session-id** *num* }

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs the advertisement switch.	**debug web-auth advertising** or **debug web-auth all**

25 Configuring Local-Account

25.1 Overview

Local-Account is a charging method used when no remote charging software is available.

- Local-Account is applicable only to scenarios in which the device serves as the PPPoE server.

Protocols and Standards

- N/A

25.2 Applications

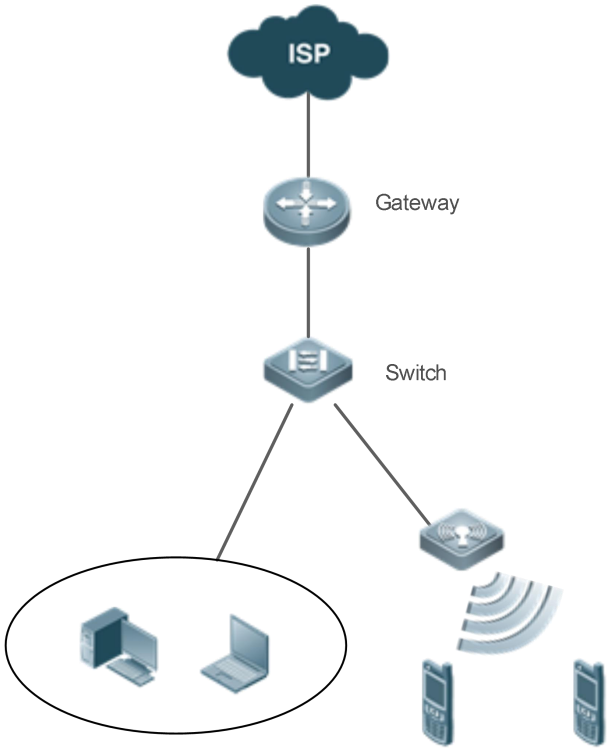
Application	Description
Configuring a Device Serving as the PPPoE Server and Implementing Local Charging	The device serves as the PPPoE server and provides the authentication and accounting services for downstream terminals and devices.

25.2.1 Configuring a Device Serving as the PPPoE Server and Implementing Local Charging

Scenario

An egress gateway is enabled with the PPPoE server function and charging function. Downstream terminals and devices are authenticated for Internet access as PPPoE clients.

Figure 25- 1



Remarks	The gateway serves as the PPPoE server and charging device.

	Downstream devices and terminals access the network as PPPoE clients.

Deployment

- Configure the egress gateway as the PPPoE server to complete client authentication.
- Configure the switch as an access device.
- Configure terminals and other network devices as PPPoE clients for authentication.
- Configure the egress gateway as the charging device to charge internal network users.

25.3 Features

Basic Concepts

PPPoE

The Point to Point Protocol over Ethernet (PPPoE) includes the PPPoE server and PPPoE client in terms of role behaviors.

Local-Account

Local-Account method is independent of an external server and charges and restricts users' Internet access behavior by the local device.

Overview

Feature	Description
User Management	Creates/Deletes valid users and assigns certain function attributes to the users.
Charging Notification System	Sends account expiration notifications in advance, and gives Internet service expiration notifications and Internet service rejection notifications.

25.3.1 User Management

The Local-Account maintains a user information database to authenticate user identities.

Working Principle

The Local-Account maintains a user information database. When a user initiates authentication via a PPPoE client, the Local-Account compares the user information with the user information and policies in the database, and determines whether to allow the user to pass authentication based on the matching result.

Creating or Deleting a User

Create or delete a user to or from the database.

Binding IP or MAC Addresses

An administrator can bind accounts with IP addresses, MAC addresses, or IP & MAC addresses according to the actual scenario.

IP-bound users can access the Internet only by using the bound IP addresses.

MAC-bound users can access the Internet only by using the bound MAC addresses.

For users configured with automatic MAC binding, the system records their MAC addresses after the users are authenticated for the first time. Then, users can be authenticated and access the Internet only by using these MAC addresses.

IP- and MAC-bound users can access the Internet only by using the bound IP and MAC addresses.

Configuring a Charging Policy

Administrators can charge users. When charging conditions are met (for example, time is up), users are prohibited from accessing the Internet.

Related Configuration

Creating or Deleting a User

Run the **local-account username** *username* command to create a user.

Use the **no** form of the **local-account username** *username* command to delete a user.

Binding IP or MAC Addresses

In local-account mode, run the **ip** *ip-address* command to bind the user account with the IP address.

In local-account mode, run the **mac** { *mac-address* / **auto** } command to bind the user account with the MAC address or configure automatic MAC address binding.

Configuring a Charging Policy

In local-account mode, run the **policy** command to configure a charging policy. Only time-based policies are supported currently.

25.3.2 Charging Notification System

The charging notification system sends account expiration notifications in advance, and gives Internet service expiration notifications and Internet service rejection notifications in the form of an HTML page. This page is displayed when a user accesses Web pages.

Working Principle

When a user's account is about to expire, the device, serving as an HTTP proxy, intercepts the user's HTTP traffic and generates a response of redirection to a preset page to remind the user.

HTTP Proxy

The HTTP proxy intercepts HTTP traffic, constructs a "notification response" packet to respond to an HTTP request, and sends it to the client.

Related Configuration

Configuring a Notification Policy

Run the **local-account notice enable** command to enable the notification function.

Run the **local-account notice date-rule** *hour interval-min* command to configure the time (in hours) in advance users are notified that their accounts are about to expire and the notification interval (in minutes).

25.4 Configuration

Configuration	Description and Command
Managing Users	(Mandatory) It is used to manage users.

	local-account user *username*	Creates a user and configures user parameters in local-account mode.
	description *string*	Configures the user description in local-account mode.
	ip *ip-address*	Binds an IP address in local-account mode.
	mac { *mac-address* / **auto** }	Binds a MAC address in local-account mode.
	policy date *yyyy mm dd*	Configures a charging policy in local-account mode.
Configuring a Charging Notification System	(Optional) It is used to notify users of their account expiration.	
	local-account notice enable	Enables the notification function.
	local-account notice date-rule *hour interval-min*	Configures a notification policy.
Configuring the Traffic Notification Interval for the Front-end Module	(Optional) It is used to notify users of their account expiration.	
	local-account period *second*	Configures the traffic notification interval (in seconds) for the front-end module.

25.4.1 Managing Users

Configuration Effect

- Add or delete users.
- Define policies for user behaviors.

Configuration Steps

Creating or Deleting a User

- Mandatory.
- The external module (for example, the PPPoE server) can use a username for authentication only after a user is configured.

Configuring User Behaviors

- Optional.

Verification

After a user is configured, a PPPoE client in the internal network can log in by using the username and password.

Related Commands

Creating a User

Command	**local-account username** *username*
Parameter Description	**username** *username*: Indicates a username.
Command Mode	Global configuration mode
Usage Guide	N/A

Binding the IP Address of the User

Command	**ip** *ip-address*
Parameter Description	**ip** *ip-address*: Indicates the IP address to be bound.
Command Mode	local-account-user mode
Usage Guide	N/A

Binding the MAC Address of the User

Command	**mac** { *mac-address* / **auto** }
Parameter Description	**mac** *mac-address*: Indicates the MAC address to be bound. **mac auto**: Indicates automatic MAC address binding.
Command Mode	local-account-user mode
Usage Guide	N/A

Configuring a Charging Policy for the User

Command	**policy date** *yyyy mm dd*
Parameter Description	**policy date**: Uses the date-based charging policy. *yyyy*: Indicates the expiration year. *mm*: Indicates the expiration month. *dd*: Indicates the expiration day.
Command Mode	local-account-user mode
Usage Guide	N/A

Configuration Example

Creating a User on the Device

Scenario	A PPPoE client is connected to the egress gateway, which is connected to an ISP network.
Configuration Steps	● Create a user named test on the device, set the user password to **test**, and bind the IP address for the user.
A	A# configure terminal A(config)# local-account user test password test ip 1.1.1.1 A(local-account-user)# ip 1.1.1.1 A(local-account-user)# mac 1111.2222.3333 A(local-account-user)# description test A(local-account-user)# policy date 2018 1 21
Verification	Run the **show local-account users web** command to display information about the created user.
A	FS#show local-account users

	(O) Online (S) State: 0=Invalid 1=Normal 3=Overdue ---------- Name O S Policy Ip addr Mac addr Note ---------- test 0 3 2018/1/21 1.1.1.1 11:11:22:22:33:33 test total:1 upper limit:150 FS

25.4.2 Configuring a Charging Notification System

Configuration Effect

- Notify a user when the account is about to expire.

Notes

- The basic functions of the Local-Account must be configured.

Configuration Steps

- Use commands to configure a charging notification system.

Verification

- Simulate a user whose account is about to expire, and check whether the user can receive notifications regularly.

Related Commands

↘ Enabling the Notification Function

Command	**local-account notice enable**
Parameter Description	**notice enable**: Enables the notification function.
Command Mode	Global configuration mode
Usage Guide	N/A

↘ Configuring a Notification Policy

Command	**local-account notice date-rule** *hour interval-min*
Parameter Description	**notice date-rule**: Sends notifications based on the expiration date. *hour:* Indicates the time in advance users are notified that their accounts are about to expire. *interval-min*: Indicates the notification interval.
Command Mode	Global configuration mode

Usage Guide	N/A

Configuration Example

Enabling the Notification Function and Configuring the Device to Give Notifications 5 Hours Before Expiration and at an Interval of 10 Minutes

Configuration Steps	● Run the following commands.
	FS# configure terminal FS(config)# local-account notice enable FS(config)# local-account notice date-rule 5 10 FS(config)# end
Verification	Run the following command to display the configuration.
	FS# show local-account config users-limit: 150 acct-period: 20s notice: on notice-time: 5h notice-interval: 10m FS#

25.4.3 Configuring the Traffic Notification Interval for the Front-end Module

Configuration Effect

- Configure the front-end module (such as the PPPoE server) to synchronize traffic information to the Local-Account module regularly.

Notes

- The basic functions of the Local-Account must be configured.
- Set the interval to a larger value for less accurate charging scenarios.

Configuration Steps

- Run commands to configure the traffic notification interval for the front-end module.

Verification

- Check the configuration and confirm that the interval is configured.
- The front-end module synchronizes traffic information to the Local-Account module regularly.

Related Commands

Enabling the Notification Function

Command	**local-account period** *second*

Parameter Description	**period** *second*: Indicates the notification interval.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Setting the Notification Interval and Enabling the Device to Give Notifications 5 Hours Before Expiration and at an Interval of 10 Minutes

Configuration Steps	● Run the following commands.
	FS# configure terminal FS(config)# local-account period 20 FS(config)# end
Verification	Run the following command to display the configuration.
	FS# show local-account config users-limit: 150 acct-period: 20s notice: on notice-time: 5h notice-interval: 10m FS#

25.5 Monitoring

Displaying

Description	Command
Displays the configuration.	show local-account config
Displays users.	show local-account users
Displays online users.	show local-account online

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs the client.	**debug local-account client**
Debugs the HTTP proxy.	**debug local-account http_proxy**
Debugs the server.	**debug local-account server**

26 Configuring the Firewall

26.1 Configuring NETWORK_DEFEND

26.1.1 Overview

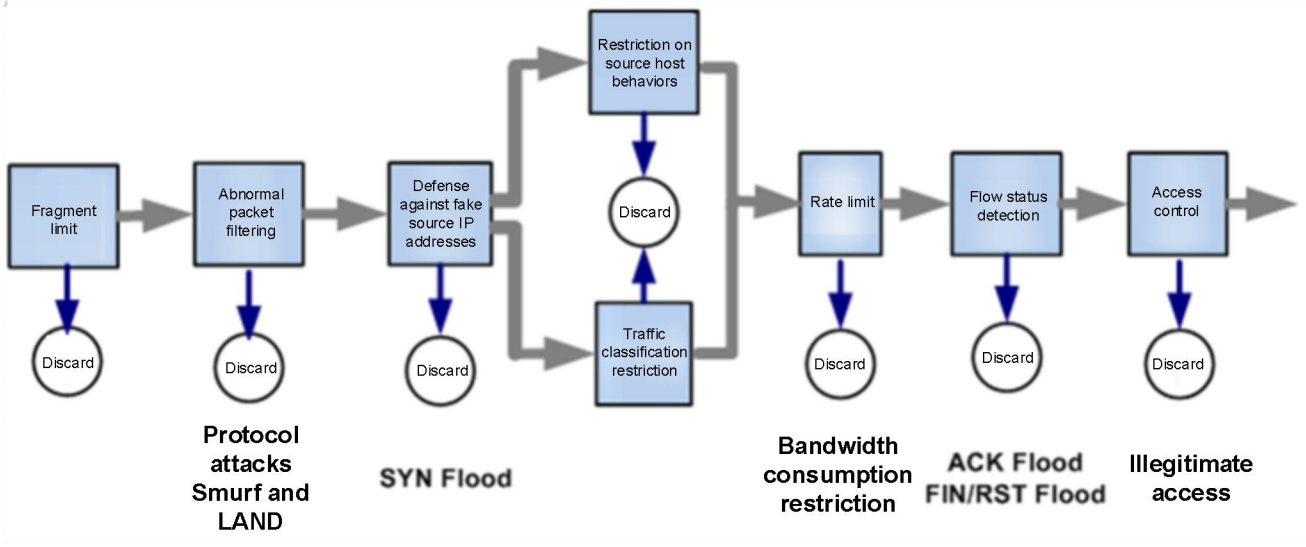
NETWORK_DEFEND of the firewall can detect multiple types of network-layer attacks and take measures to protect the internal network against malicious attacks, thereby ensuring normal running of the internal network and system.

NETWORK_DEFEND of the firewall is advantageous in the following aspects:

- It can defend against all types of network-layer attacks.
- The conventional method of configuring Access Control Lists (ACLs) on switches or routers has limitations in traffic filtering and attack detection. The ACLs are unable to filter out all types of attack traffic and cannot properly solve the filtering problem in the case of stateful connections. The combination of the firewall and ACL is an effective solution.
- The stateful firewall tracks the session initialization and status. By checking data packet headers, the stateful firewall analyzes and monitors the network layer (layer-3) and protocol layer (layer-4) to allow, reject, or forward network traffic according to user-defined firewall policies.
- The stateful firewall identifies attack behaviors based on the traffic behavior characteristics, and specifically isolates malicious traffic.
- The firewall classifies protection domains based on subnets or IP address sets, independently conducts traffic monitoring, analysis, policy implementation, and generates a detailed attack report for each protection domain.

The figure below shows the attack filtering model.

Figure 266- 1



Each network attack defense domain has an independent defense system. Traffic passing through the firewall is transmitted to independent network attack defense domains so that malicious traffic is isolated. You can configure a bypass traffic policy to bypass the attack defense system.

The firewall adopts a multi-layer model to filter out malicious traffic. It detects and filters packets by layer to identify and isolate malicious traffic. The source IP anti-forgery function is an important part of NETWORK_DEFEND. It classifies packets into packets with authentic source addresses and packets with untrusted source addresses for processing. For packets from authentic source hosts, the function module further tracks the behaviors of the source hosts to identify attacks from the authentic source hosts. For packets with untrusted source addresses, the function module limits and even discards the packets.

Rate limit is applied to valid traffic so as to prevent early discarding of valid traffic.

The access control function of the firewall can be implemented by the ACL and security zone component.

NETWORK_DEFEND described in this document supports only the IPv4 protocol.

26.1.2 Applications

Application	Description
Security Threats and Attack Defense of the Server Area	Protects the server against attacks from internal and external networks.
Security Threats and Attack Defense of the Internal Network	Monitors and defends against attacks from the internal network, such as virus spreading.

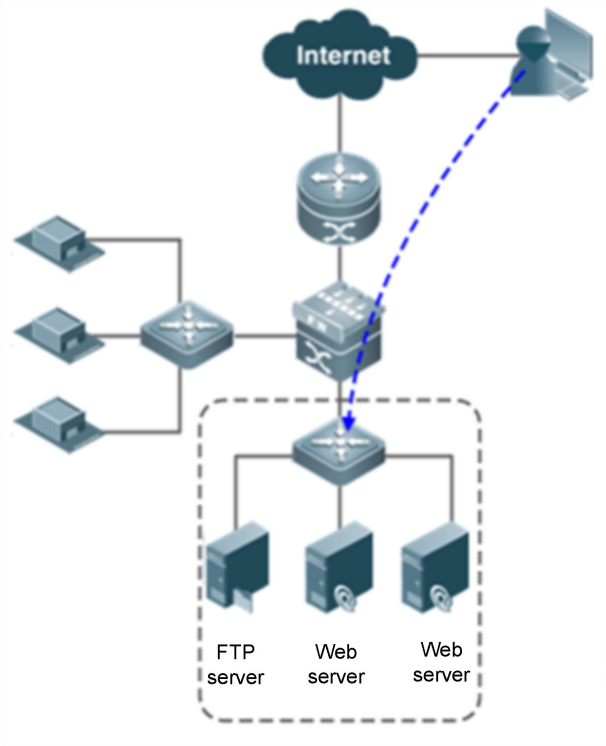
26.1.2.1 Security Threats and Attack Defense of the Server Area

Scenario

User servers open to the Internet are attacked very commonly. Server area attacks initiated from the Internet may keep the servers busy and paralyzed. As a result, the servers fail to provide services normally. Server attacks are mainly resource-consuming attacks. Attackers control puppet hosts on the Internet to conduct Distributed Denial of Service (DDoS) attacks (such as SYN Flood, ICMP flood, and CC attacks) on the server area (usually Web servers). SYN flood attacks are the most common type of attack. Attackers usually use forged source IP addresses to initiate such attacks. Therefore, it is difficult to identify, track, and defend against such attacks. In addition, attackers can conduct SYN flood attacks at a low cost but the attacks will consume considerable resources.

To defend against such attacks, you can enable the policy of defending against resource-consuming attacks on the firewall, to prevent such attacks from reaching the server area.

Figure 266- 2



Deployment

Egress gateway

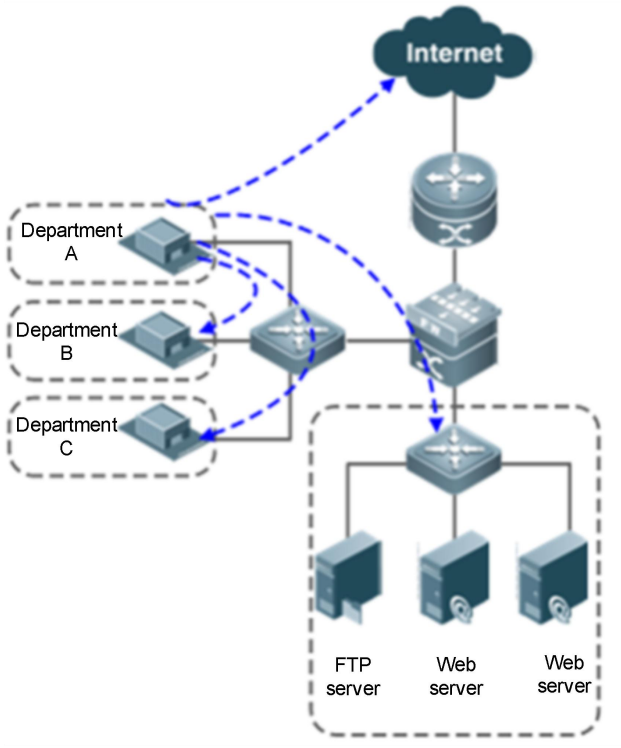
- Deploy an egress gateway at the network egress so that all traffic bound for the server area is filtered by the egress gateway.
- Allocate a network attack defense domain to the network segment, to which the server area belongs, and deploy a dedicated defense policy. In this way, the egress gateway checks data transmitted to the server area, defends against attacks, and generates attack reports.
- Enable the egress gateway to monitor the continuous traffic of servers in the network attack defense domain and record the traffic situation.

26.1.2.2 Security Threats and Attack Defense of the Internal Network

Scenario

Network attacks confronting the internal network usually include resource-consuming attacks, network snooping attacks, and worm and virus spreading attacks. Attacks conducted by internal network users on the internal network are more damaging. Once the worms and viruses outbreak or attackers intentionally sniff network information to find out vulnerabilities, the security of the internal network will be greatly challenged and affected.

Figure 266- 3



Deployment

Egress gateway

- Deploy an egress gateway at the network egress so that all traffic bound for the internal network is filtered by the egress gateway.
- Specify the network attack defense domains to be protected and monitored and deploy ingress/egress defense policies for the domains, for example, deploy an anti-scanning policy in the outbound direction.
- Enable the egress gateway to detect the traffic that enters or leaves each network attack defense domain, defend against attacks, and generate attack reports.

26.1.3 Features

Basic Concepts

Network Attack Defense Domain

A network attack defense domain is a collection of hosts and subnets sharing the same protection policy. Devices in a network can be allocated to network attack defense domains to facilitate the network defense deployment and configuration. Different domains can be independently managed.

Defense Policy Self-learning

The policy self-learning function can be enabled for a network attack defense domain, so as to collect daily service data of the domain, and thus obtain data reference values of normal services. Administrators can, based on the data reference values, derive a threshold for identifying abnormal traffic, by using a certain multiple. The self-learning function helps administrators deploy more appropriate protection policies on the basis of better understanding of their service status.

Source Verification

The first step of identifying an attack is to check whether the source IP address of packets is faked. The process of distinguishing packets with faked source IP addresses is called source verification. The **auth** and **unauth** keywords are used to classify and process traffic based on different results of source verification. The TTL identification and TCP proxy methods can be used to check the authenticity of source hosts.

It is difficult to judge whether all packets are from authentic source IP addresses. In some cases, for example, when a host accesses a network attack defense domain for the first time and the packets are not TCP packets, the source IP addresses of the packets cannot be judged and such packets are classified as the unauth type. Users are recommended to limit the traffic of the unauth type rather than discard all of it. A better method is to adopt policy learning to obtain a proper classification proportion.

Overview

Feature	Description
NETWORK_DEFEND Enabling	Enables the NETWORK_DEFEND function and deploys the protection mode.
Defense Against Protocol Attacks	Defends against LAND, Smurf, and Fraggle attacks.
Global Protection	Deploys a policy for all traffic that passes through the firewall to prevent resource depletion of network devices.
Domain-based Protection	Configures a network attack defense zone, and deploys policy learning and accurate network defense in the zone.

26.1.3.1 NETWORK_DEFEND Enabling

NETWORK_DEFEND provides protection on the universal platform. You can deploy the protection mode based on the application scenario.

Working Principle

NETWORK_DEFEND provides network protection for devices. After the function is enabled, it can defend against protocol attacks and provide global protection and domain-based protection for devices according to deployed policies. If Network Address Translation (NAT) is deployed on the network, the NETWORK_DEFEND mode needs to be set to NAT mode.

Related Configuration

NETWORK_DEFEND is disabled by default. It works in non-NAT mode by default.

Run the **net-defend enable** command to enable NETWORK_DEFEND or use the **no** form to disable the function.

Run the **net-defend mode** command to switch the work mode of NETWORK_DEFEND.

26.1.3.2 Defense Against Protocol Attacks

In protocol attacks, an attacker, by utilizing vulnerabilities in protocol stack implementation on the target device, sends specific traffic or packets (deformed packets) to make the target device become abnormal, achieving Denial of Service (DoS). Common protocol attacks include the Local Area Network Denial (LAND) attacks, Smurf attacks, Fraggle attacks, TearDrop attacks, WinNuke attacks, abnormal TCP flags, ICMP redirection attacks, ICMP destination unreachable attacks, and jumbo ICMP packet attacks.

Working Principle

Protocol attacks mainly target at protocol processing vulnerabilities. Relevant functions can be configured to filter out packets with attack characteristics.

LAND

Attack principle/characteristics: The source address and destination address in data packets used for LAND attacks are the same. The protocol stack design in early OSs is defective. When such an OS receives LAND attack packets, the OS may do not know how to handle packets with the same source and destination addresses in the stack or may cyclically send and receive the packets, consuming considerable system resources and even causing system breakdown or crash.

Smurf

Attack principle/characteristics: In Smurf attacks, an attacker sends a packet with a specific request (for example, ICMP echo request) to the broadcast address of a subnet and disguises the source address as the host address to be attacked. Each host in the subnet responds to the broadcast packet and sends a packet to the attacked host, causing the host to be attacked. The attack can, at a low cost, cause heavy attack traffic to the attacked host.

Fraggle

Attack principle/characteristics: Fraggle attack is a revision to the Smurf attack. Fraggle attacks use UDP responses rather than ICMP packets to attack port 7 (echo) or port 19 (chargen).

WinNuke

WinNuke attacks are also called out-of-band (OOB) transmission attacks, which are characterized by the attack on a target port. The attacked target port is usually port 139 and the URG bit is set to 1, indicating emergency mode. In WinNuke attacks, an attacker utilizes a vulnerability of the Windows OS to send some packets that carry TCP OOB data to the attacked port. These attack packets, however, are different from normal packets that carry OOB data, and the pointer fields do not match the actual position of data, that is, overlapping exists. The Windows OS will break down when processing these packets. The configuration below can be adopted to effectively defend against such attacks.

ICMP Redirection Attack

Attack principle/characteristics: When a host uses the non-optimal route to send data packets, the device sends an ICMP redirection packet to notify the host of the optimal route. In general, the device sends the ICMP redirection packet only to the host, but some malicious attacks may span a network segment and the attacker sends false redirection packets to hosts in another network. The ICMP redirection attack is intended to change the routing table of hosts, damage the routing, and disturb normal IP packet forwarding of hosts, thereby enhancing the eavesdropping capability.

Attack Using IP Packets That Carry the Source Routing Option

Attack principle/characteristics: The IP protocol adds option fields to the IP packet header to implement some auxiliary functions. The fields can carry some data selectively to instruct the intermediate or final target PC to process these IP packets additionally. The source routing option is one of the fields.

The source routing option is used to instruct the intermediate device how to forward data packets, that is, clearly specify the packet transmission path. For example, to explicitly enable an IP packet to pass through three devices: R1, R2, and R3, you can specify the port addresses of the three devices in the source routing option. Then, the IP packet will pass through R1, R2, and R3 in sequence regardless of the routing tables on the three devices. In addition, the source address and destination address of IP packets with the source routing option change all the time during transmission. Therefore, by setting the source routing option properly, an attacker can forge some valid IP addresses to send attack packets to the network.

Related Configuration

By default, LAND attack defense and Smurf attack defense are enabled. No configuration command is available to disable the Smurf attack defense function.

Run the **defend** command to enable or disable the protocol attack defense.

The protocol attack defense is configured independently and imposes no impact on other attack defense commands.

The defense against protocol attacks is prior to global protection and domain-based protection.

26.1.3.3 Global Protection

Global protection is provided for the entire firewall, to prevent firewall DoS caused by resource-consuming attacks. In global protection, the session rate is limited on the entire firewall to ensure that resources of the firewall are effectively utilized.

Working Principle

A network attack defense domain is used to provide protection for a specific area. The firewall can be divided into multiple domains. When attack traffic is not destined for a specific domain or attack traffic has no fixed target, the attack traffic out of the coverage of policies will consume bandwidth of the entire network. If there are a large number of forged attack packets, relevant resources of network devices including the firewall will be depleted, and the devices fail to provide normal services.

Global protection can be configured on the firewall to defend against such attacks. The TCP SYN cookie function can filter out TCP SYN flood attack packets. The session limit function can filter out suspicious attack packets from new sessions and limit the transmission rate of these suspicious packets, so as to isolate malicious traffic and protect the service of the firewall.

The firewall defines the following new sessions as sessions that do not pass verification:

1. TCP sessions that do not pass verification of the TCP source address anti-forgery technology (SYN-cookie).
2. Non-TCP new sessions, in which the number of hops (TTL) from the initiator to the firewall is suspicious.

Therefore, after global protection is configured, all TCP sessions from authentic source addresses are free from interference. On the contrary, non-TCP sessions are affected by the TTL learning of the firewall.

Related Configuration

Global protection needs to be disabled when the firewall performance and capacity are tested. Run the **defend-zone global** command to enable global protection.

Global protection is prior to the network attack defense domain function.

In global protection, the policy priority is as follows: the rate limit for creation of sessions that do not pass verification is prior to the rate limit for UDP, TCP, ICMP, and other protocol sessions.

The default threshold of global protection is high and therefore it only ensures the normal running of the firewall. Users can enable policy self-learning to obtain reasonable policy configuration suggestions. The policy self-learning is similar to that in attack defense domains.

26.1.3.4 Domain-based Protection

Network attack defense domains are configured to classify and protect hosts and subnets in the network and manage them independently. Different host objects can use different protection policies and can be maintained and managed by different administrators.

Working Principle

Configuring a Network Attack Defense Domain

Users can allocate hosts and subnets to independent network attack defense domains and deploy specific policies for the domains. Domains are controlled independently of each other, and policy learning and policies can be deployed on the domains.

Configuring Policy Self-learning

Before configuring a defense policy, users can enable the policy self-learning function. By monitoring traffic for a period of time, the device provides reasonable policy configuration suggestions for the network attack defense domain. Users cannot enable the manually configured defense policies during policy learning. Therefore, if the system is attacked during policy learning (for example, an abnormality occurs when a network attack defense domain is suspected to be attacked), the policy thresholds learned by the system are inaccurate. In this case, users are recommended to restart policy self-learning. The policy learning duration should be 7 days or longer.

Policy suggestions provided via policy learning are obtained based on traffic peaks in a network attack defense domain during monitoring. Users can directly use these thresholds or adjust them, for example, increase the thresholds by a certain percentage.

Configuring Traffic Monitoring

Users often do not know how to configure targeted network protection measures and thresholds for the local network attack defense domain when conducting security policy protection on the network. Before security policies are carried out, the traffic of a network attack defense domain can be monitored to better help users work out effective protection measures.

After setting protection measures, users can compare traffic monitoring results to determine the protection effect. By means of traffic monitoring, users can identify suspicious hosts and take targeted measures to handle these suspicious hosts.

Users are recommended to monitor the traffic of a network attack defense domain in 7x24 mode before protection policies are applied to the network attack defense domain. This helps users define a more reasonable threshold range.

The firewall can monitor real-time/history peak traffic and average traffic of different protocol modules. It can display the TopN source hosts with relevant characteristics based on TCP packets. In this way, users can know the traffic status of each protected host and rapidly handle suspicious cases.

⚠ Traffic monitoring degrades the device performance, and therefore it is disabled by default. After relevant security policies work properly, users can disable traffic monitoring to ensure the maximum service processing capability of devices.

Configuring Attack Defense Policies

Users can deploy defense policies on a network attack defense domain to defend against various types of attacks.

- Dynamic defense policy: Defends against resource-consuming attacks, worms, and network snooping attacks. Such policies provide dynamic protection based on real-time changes of traffic. Attack defense reports will be generated.

⚠ The device automatically prolongs the protection provided by dynamic defense policies based on attack continuity. For example, if an attack lasts one hour, the dynamic protection will also last one hour after the attack is detected. Dynamic protection will continue for the timeout time specified in the policy one hour after the attack has been stopped.

⚠ The device, on which the protection policy of "drop" or "blocking" is deployed, may fail to monitor whether the attack is underway. Therefore, such a policy will be stopped after the timeout time specified in the policy expires. If the attack is still in progress, the policy will provide the same protection. In this case, multiple attacks are recorded in the attack report.

Attack traffic can be classified into two types: attack traffic with fake source IP addresses and attack traffic with authentic source IP addresses. For the former, an attacker does not need to receive responses from victims, such as TCP SYN flood attacks. For the latter, an attacker uses numerous application service requests and concurrent connections to deplete host resources. The anti-forgery mechanism enables the firewall to isolate fake traffic. For traffic from authentic source IP addresses, the firewall limits host behaviors by limiting the connection mode, to prevent risks to hosts in the domain.

Dynamic defense policies are capable of defending against the following types of attacks:

(1) Attacks using fake source IP addresses

For TCP traffic, the TCP SYN cookie mechanism can be used to isolate fake traffic to ensure that TCP traffic bound for the domain is from authentic IP addresses. If an authentic source host sends non-TCP traffic to a network attack defense domain before completing the three-way handshake with a host in the network attack defense domain, such traffic may not pass the authentic source IP address verification. Once the host completes the three-way handshake with a host in the network attack defense domain, non-TCP traffic from this host can pass the authentic source IP address verification. Traffic that does not pass authentic source verification can be discarded or limited to reduce risks to hosts in network attack defense domains.

(2) Attacks using authentic source IP addresses

The device with dynamic defense policies deployed collects statistics on data of authentic hosts to identify behavior abnormalities of hosts, such as abnormal number of concurrent connections and scanning behavior.

(3) Connection depletion attacks

An attacker can deplete TCP connections of the server to cause the server DoS. Policies can be deployed on the firewall to identify such attacks and take pertinent defense measures.

(4) Scanning attacks

An attacker can use a scanning tool to probe the target address/target service, to find out target systems/services that exist and are connected to the target network. If a host gives a response, it indicates that the address/service exists. By scanning, the attacker can find out the target hosts/services for attacks. All PCs connected to the network run many services that use the TCP/UDP port. Scanning helps attackers find out the ports that can be used for attacks. Attackers usually use the ICMP protocol to scan hosts and use the TCP protocol to scan ports. In essence, port scanning is to send a message to each port and only one message is sent each time. The type of received responses indicates whether a port is used and an attacker can probe the port to find out its vulnerabilities. Port scanning is usually conducted on connection-oriented TCP ports. Therefore, attackers will obtain effective feedback. The scanning detection function of NETWORK_DEFEND can track behaviors of hosts that access network attack defense domains, to determine whether host behaviors meet scanning characteristics, so as to check whether a host is scanning.

- Static defense policy: Includes the blacklist, bypass traffic policy, packet rate limit policy of hosts, and session creation rate limit of hosts.

  The packet rate limit function of hosts allows users to limit the traffic that enters or leaves network attack defense domains for each host, so as to protect host resources against excessive consumption.

  The session creation rate limit function of hosts allows users to limit the creation rate of sessions that enters or leaves network attack defense domains for each host, so as to protect host resources against excessive consumption.

  Users can define a blacklist to block specified traffic that is to enter or leave network attack defense domains.

  Users can configure a bypass traffic policy to exempt some traffic from network attack defense detection.

Recording Logs

When the system is attacked, users can run the **show defend-zone net-defend-zone-name running-protect** command to display the underway attack event. If no real-time tracking is available, you can enable the log function to record completed attacks into the database. Then, you can view history attack events.

Related Configuration

Configuring a Network Attack Defense Domain

By default, the firewall does not automatically classify network attack defense domains.

Run the **defend-zone** command to configure a network attack defense domain.

The domain-based policy self-learning and policy deployment can be implemented only after a network attack defense domain is configured.

⚠ When the NAT function is enabled on the egress gateway, if the attack defense function is deployed, IP addresses before and after NAT translation need to be added to the attack defense domain. In addition, the internal IP network segment corresponding to the NAT external IP network segment needs to be added to the attack defense domain. For example, the NAT internal IP address segment is 192.168.1.0/24 and the corresponding NAT external IP address segment is 110.249.191.0/30. Both network segments need to be added to the IP address range to be protected in the attack defense domain.

Configuring Policy Self-learning

After a network attack defense domain is created, the device does not conduct policy self-learning automatically.

Run the **net-defend learning** command to enable policy self-learning of a specified network attack domain.

The policy self-learning must be performed prior to policy deployment.

Configuring Traffic Monitoring

By default, traffic monitoring is not performed on network attack defense domains.

You can run the **traffic-monitor** command to enable traffic monitoring.

Traffic monitoring and attack defense policies can be deployed simultaneously.

Configuring Attack Defense Policies

By default, no attack defense policy is deployed in network attack defense domains.

(1) Dynamic attack defense policy

An attack defense policy consists of the following elements:

"Policy type" + "traffic characteristics" + "monitored object" + "threshold" + "minimum effective duration" + "action"

The policy is interpreted as follows:

This is a policy of the **policy type**. When a **traffic characteristic** of a **monitored object** exceeds the **preset**, relevant **action** must be taken and the action execution time is not shorter than the **minimum effective duration**.

- Policy type

Keyword	Description
tcp-auth	Indicates a policy applicable to all TCP service traffic from authentic source IP addresses.
tcp-unauth	Indicates a policy applicable to all TCP service traffic that does not pass authentic source verification.

icmp	Indicates a policy applicable to ICMP traffic.
udp	Indicates a policy applicable to UDP traffic.
other-protocol	Indicates a policy applicable to IP traffic other than TCP, UDP, and ICMP traffic.
scan	Indicates a policy applicable to scanning behavior traffic.

- Traffic characteristics

Keyword	Description
syns-in	Indicates the rate of TCP SYN packets that enter a network attack defense domain.
half-conn-in	Indicates the number of incomplete TCP handshake connections initiated to a network attack defense domain.
conn-in	Indicates the number of TCP connections initiated to a network attack defense domain.
pkt-in	Indicates all types of packets that enter a network attack defense domain.
pkt-out	Indicates all types of packets that leave a network attack defense domain.
unauth-src-in	Indicates packets that enter a network attack defense domain but do not pass authentic source verification.
auth-src-in	Indicates packets that enter a network attack defense domain and are from authentic source hosts.

- Monitored object

Keyword	Description
dst-ip	Indicates that monitoring is conducted on destination hosts. This type of policy is applied to the inbound direction. It can be understood that monitoring is conducted on each host inside a network attack defense domain.
src-ip	Indicates that monitoring is conducted on each source host. This type of policy is applied to the inbound direction. It can be understood that monitoring is conducted on each source host outside a network attack defense domain.
global	Indicates that monitoring is conducted on all traffic that enters a network attack defense domain.

- Threshold

This field indicates the threshold for triggering an attack defense policy. Different threshold units can be configured for different policies.

- Minimum effective duration

This field is optional. It indicates the minimum effective duration of a triggered attack defense policy. The default value is 60 seconds and the duration can be adjusted. Defense policies are always effective before an attack is stopped.

- Action

Keyword	Description
anti-spoofing	Defends against traffic with fake source IP addresses.
limit	Limits traffic according to the threshold.
blocking	Blocks all traffic from a specified host.
drop	Discards traffic specified in policies.
notify	Records attack behaviors only.

(2) Static attack defense policy

Run the **ratelimit** command to configure the rate limit.

Run the **bypass** command to configure a bypass traffic policy.

Run the **blacklist** command to configure a blacklist.

(3) Policy priorities (in descending order)

1) Bypass traffic policy (bypass)

2) Black (blacklist)

3) Protection policy for TCP, UDP, ICMP, and other protocol packets

4) Rate limit policy for host packets (rate-limit)

5) Protection policy for TCP, UDP, ICMP, and other protocol sessions

6) Rate limit policy for host session creation (session-limit)

In the same protocol protection policy, the "global" monitored object is prior to the "src-ip" and "dst-ip" monitored objects, and packet-based filtering is prior to connection quantity-based filtering.

Recording Logs

By default, the firewall does not log any attacks.

Run the **log** command to enable the log function. Attacks initiated afterwards will be recorded in the local database of the device. You can run the **show defend-zone** *net-defend-zone-name* **report** command on the egress gateway to display logs. The system records logs of seven days at most.

26.1.4 Configuration

Configuration	Description and Command	
Configuring Defense Against Protocol Attacks	(Optional) It is used to configure defense against protocol attacks.	
	defend	Enables defense against protocol attacks.
Configuring a Network Attack Defense Domain	(Optional) It is used to configure a domain for accurate attack defense.	
	defend-zone	Creates a network attack defense domain.
	description	Configures a description for the network attack defense domain.
	ip access-group	Configures an ACL associated with the network attack defense domain.
	net-defend learning	Enables defense policy learning.
	(Optional) It is used to configure defense policies for the network attack defense domain.	
	tcp-unauth	Enables the protection policy for TCP traffic that does not pass the source verification.
	tcp-auth	Enables the protection policy for TCP traffic that passes the source verification.
	udp	Enables the protection policy for UDP traffic.
	icmp	Enables the protection policy for ICMP traffic.

	other-protocol	Enables the protection policy for traffic other than the TCP, UDP, and ICMP traffic.
	ratelimit	Limits the rate of specific traffic.
	session-limit	Limits the creation rate for specific sessions.
	bypass	Configures a bypass traffic policy.
	blacklist	Configures a blacklist.
Configuring Global Protection	(Optional) It is used to classify and limit the traffic that passes through the firewall to prevent DoS attacks occurring on network devices. By default, global protection is enabled on the firewall but disabled on the egress gateway.	
	defend-zone global	Enables global protection.
	net-defend learning	Enables defense policy learning.
	tcp	Configures the global TCP SYN cookie proxy.
	session-limit	Configures the global rate limit for session creation.
Enabling NETWORK_DEFEND	(Mandatory) It is used to enable NETWORK_DEFEND, which is disabled by default.	
	net-defend enable	Enables NETWORK_DEFEND.
	(Optional) It is used to configure the NETWORK_DEFEND mode, which is non-NAT mode by default.	
	net-defend mode { nat | no-nat }	Configures the NETWORK_DEFEND mode.

26.1.4.1 Enabling NETWORK_DEFEND

Configuration Effect

Enable NETWORK_DEFEND function and set the work mode.

Configuration Steps

Enable NETWORK_DEFEND in global configuration mode as required. Set the work mode for NETWORK_DEFEND based on the deployment scenario.

Verification

Initiate attacks and check whether the attacks are intercepted by the egress gateway.

Related Commands

Enabling NETWORK_DEFEND

Command	net-defend enable
Parameter Description	N/A
Command Mode	Egress gateway: Global configuration mode
Usage Guide	NETWORK_DEFEND is disabled by default. Enable NETWORK_DEFEND in global configuration mode. In addition, be

	sure to run the **ip session tcp-state-inspection-enable fw** and **ip session track-state-strictly** commands. When NETWORK_DEFEND is disabled, you also need to disable the **ip session tcp-state-inspection-enable fw** and **ip session track-state-strictly** commands.

Configuring the NETWORK_DEFEND Mode

Command	net-defend mode { nat | no-nat }
Parameter Description	**nat**: Indicates NAT mode. **no-nat**: Indicates non-NAT mode.
Command Mode	Egress gateway: Global configuration mode
Usage Guide	The default NETWORK_DEFEND mode is NAT mode on a gateway and non-NAT mode on a bridge. If NAT is deployed on the network, the NETWORK_DEFEND mode needs to be set to NAT mode. A bridge does not support NAT and NAT mode cannot be configured on it.

Configuration Example

Enabling NETWORK_DEFEND

Configuration Steps	● Run commands to enable NETWORK_DEFEND on the egress gateway.
A	A# configure terminal Enter configuration commands, one per line. End with CNTL/Z. A(config)# net-defend enable A(config)# net-defend mode nat A(config)# exit
Verification	● Run the **show running** command to display the configuration.

26.1.4.2 Configuring Defense Against Protocol Attacks

Configuration Effect

Filter out various types of attack packets, including LAND, Smurf, Fraggle, TearDrop, WinNuke, abnormal TCP tag, ICMP redirection, ICMP destination unreachable, and jumbo ICMP attack packets.

Configuration Steps

In global configuration mode, configure required commands for defending against specific attacks on the current firewall.

Verification

Initiate attacks and check whether attack packets are intercepted by the firewall.

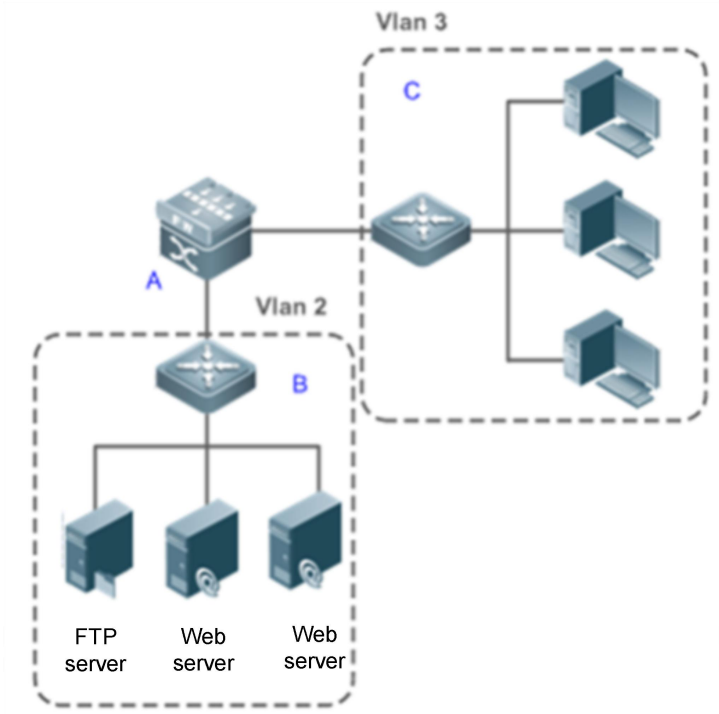
Related Commands

Command	defend { winnuke | source-route | route-record | icmp-unreachable | fraggle | land | large-icmp [*icmp-length*] }
Parameter Description	*Icmp-length*: Indicates the allowable ICMP packet length, in bytes. The value ranges from 28 to 65,535. If *icmp-length* is not set, the default value **4000** is used.

Command Mode	Egress gateway: Global configuration mode
Usage Guide	This command is used to enable the defense against various types of protocol attacks.

Configuration Example

Filtering Out Protocol Attack Packets on the IPv4 Network

Scenario Figure 266-4	
Configuration Steps	● Configure relevant commands for defending against protocol attacks on the egress gateway.
A	A# configure terminal Enter configuration commands, one per line. End with CNTL/Z. A(config)# defend winnuke A(config)# defend source-route A(config)# defend route-record A(config)# defend icmp-unreachable A(config)# defend fraggle A(config)# defend land A(config)# defend large-icmp A(config)# exit
Verification	● Enable a host to send a data packet with the same source and destination IP addresses. Verify that the data packet is intercepted when it passes through the egress gateway.
A	A# show defend drop Drops packet: 5

	Land: 5

26.1.4.3 Configuring Global Protection

Configuration Effect

Limit the rate of sessions that pass through the firewall/egress gateway to prevent resource depletion of network devices.

Configuration Steps

Run the **defend-zone global** command in global configuration mode, and configure rate limit policies in config-defend-global mode.

Verification

Initiate attacks and check whether attack packets are intercepted by the firewall/egress gateway.

Related Commands

Entering Global Attack Defense Configuration Mode

Command	defend-zone global
Parameter Description	N/A
Command Mode	Egress gateway: Global configuration mode
Usage Guide	This command is used to enter the global attack defense configuration mode.

Enabling Policy Learning for Global Protection

Command	net-defend learning global [days days]
Parameter Description	days: Indicates the number of policy learning days. The value ranges from 3 to 60 and the default value is **7**.
Command Mode	Privileged EXEC mode
Usage Guide	Global protection is enabled by default. The default threshold of global protection is high and therefore it only ensures the normal running of the firewall. Users can enable policy self-learning to obtain reasonable policy configuration suggestions. The policy self-learning is similar to that in attack defense domains. It is recommended to raise policy thresholds obtained via policy learning by a certain percentage (for example, by 50% or 100%) and then apply these thresholds. The purpose is to prevent normal traffic from being mistakenly judged as attack traffic and thereby being blocked.

Configuring Defense Against TCP SYN Flood Attacks

Command	tcp { syns-in | half-conn-in } global threshold threshold-num action anti-spoofing
Parameter Description	threshold-num: When **syns** is set, it indicates the maximum number of packets per second (pps) and the value ranges from 1 to 800,000. When **half-conn** is set, it indicates the maximum number of semi-connections and the value ranges from 1 to 10,000,000.

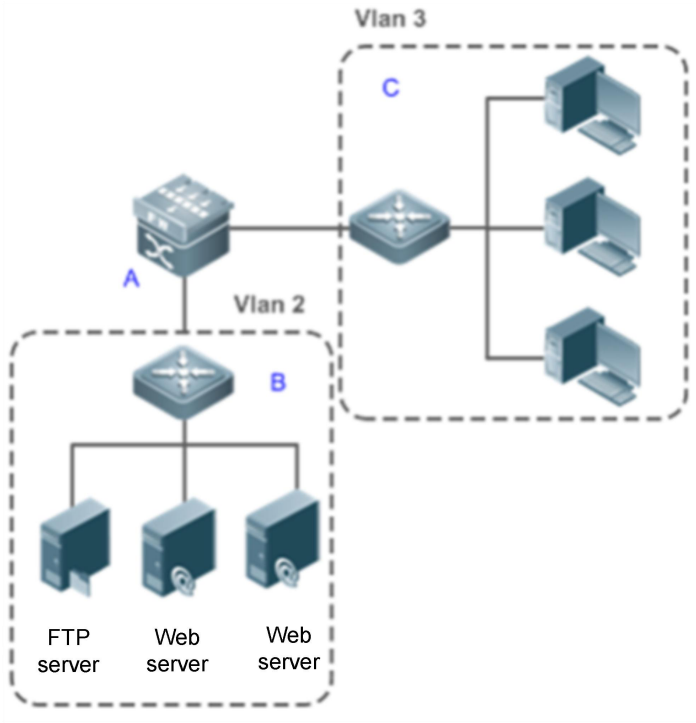
Command Mode	config-defend-global
Usage Guide	This command is used to enable attack defense when the rate of SYN packets that pass through the firewall exceeds the threshold or the number of TCP semi-connections exceeds the threshold.

Limiting the Creation Rate of Various Sessions

Command	session-limit { unauth-src-new-session | tcp | udp | icmp | other-protocol } new-session-per-second
Parameter Description	unauth-src-new-session: Limits the creation rate of all sessions that do not pass the source verification. tcp: Limits the creation rate of all TCP sessions. udp: Limits the creation rate of all UDP sessions. icmp: Limits the creation rate of all ICMP sessions. other-protocol: Limits the creation rate of all IP sessions other than the TCP, UDP, and ICMP sessions. new-session-per-second: Indicates the number of sessions created per second. The value ranges from 1 to 1,000,000.
Command Mode	config-defend-global
Usage Guide	This command is used to limit the creation rate of various sessions. The limit on traffic that does not pass the source verification is prior to the limit on other types of traffic. When the traffic of a new non-TCP session reaches the firewall, if the firewall has not learned the TTL of the network segment to which the source IP address of the non-TCP new session belongs, the firewall classifies the session traffic as the traffic that does not pass source verification, and limits the session creation. When the firewall detects the TCP three-way handshake from any host in the same network segment as the non-TCP new session, the firewall can learn the TTL of the network segment and removes the limit above. To reduce TTL misjudgment, you are recommended to set **new-session-per-second** to a larger value when configuring the **session-limit** command, and then reduce the value after the device learns the TTL for about one week. Global protection can provide continuous protection service when the firewall processes a large amount of attack traffic. If an attack is targeted at the firewall and the firewall configuration management is delayed consequently, the Network Foundation Protection Policy (NFPP) must be configured.

Configuration Example

Enabling Global Protection

Scenario Figure 266- 5	
Configuration Steps	● Configure relevant global protection commands on the egress gateway.
A	A# configure terminal Enter configuration commands, one per line. End with CNTL/Z. A(config)# defend-zone global A(config-defend-global)# tcp half-conn-in global threshold 1000 action anti-spoofing A(config-defend-global)# exit
Verification	● Enable a host to send TCP SYN packets that exceeds the preset threshold. Verify that packets that fall outside the threshold are intercepted by the egress gateway.
A	A# show defend drop Drops packet: 102 Global protect: 102

Common Errors

- No appropriate threshold is set. It is recommended to set the threshold to a larger value and then gradually reduce it based on the actual situation.
- When dual firewall service modules are inserted into the core switch, the values of all restriction parameters for global protection are reduced by half on each service module. For example, the UDP session creation rate set by users is no more than 10,000 sessions per second. Then, the session creation rate does not exceed 5,000 sessions per second on each firewall service module.

26.1.4.4 Configuring a Network Attack Defense Domain

Configuration Effect

- Provide independent protection for hosts in an area.
- Provide the dynamic policy self-learning function.
- Defend against various types of attacks.
- Provide refined traffic monitoring.
- Specify a bypass traffic policy and blacklist manually.
- Set the host rate limit.
- Provide complete attack reports.

Notes

- Dynamic policy self-learning cannot be simultaneously configured with other attack defense policies.

Configuration Steps

- Create a network attack defense domain.
- Enable policy self-learning.
- Deploy attack defense policies.

Verification

- Check the status of the network attack defense domain.
- Enable a device to send attack packets to the network attack defense domain.
- Check packet statistics and intercepted packets of the network attack defense domain.

Related Commands

Creating a Network Attack Defense Domain

Command	defend-zone net-defend-zone-name
Parameter Description	net-defend-zone-name: Indicates the name of a network attack defense domain.
Command Mode	Egress gateway: Global configuration mode
Usage Guide	This command is used to create a network attack defense domain.

Configuring a Description for the Network Attack Defense Domain

Command	description description-string
Parameter Description	description-string: Indicates the description of the network attack defense domain. It can contain a maximum of 100 characters.
Command Mode	Network attack defense domain configuration mode
Usage Guide	This command is used to configure a description for the network attack defense domain.

Associating an ACL

Command	ip access-group access-list
Parameter Description	access-list: Indicates the name of the associated standard ACL.
Command Mode	Network attack defense domain configuration mode
Usage Guide	This command is used to associate an ACL to specify the scope of the network attack defense domain. ⚠ If the ACL to be associated does not exist or is incorrect, this command is still available but an error prompt will be displayed. Users need to manually correct the ACL association. The association with an incorrect ACL will invalidate the function. Run the **show defend-zone web** command to display the attack defense status. ⚠ The ACL associated with attack defense can contain no more than 200 ACEs. Only the ACL composed of **access-list id permit {src src-wildcard | host src }** ACEs is supported. When the associated ACL does not meet this condition, the network attack defense domain is unavailable. The deny policy and the **any** and **time-range** keywords are not supported in ACLs. ⚠ When the NAT function is enabled on the egress gateway, if the attack defense function is deployed, IP addresses before and after NAT translation need to be added to the attack defense domain. In addition, the internal IP network segment corresponding to the NAT external IP network segment needs to be added to the attack defense domain. For example, the NAT internal IP address segment is 192.168.1.0/24 and the corresponding NAT external IP address segment is 110.249.191.0/30. Both network segments need to be added to the IP address range to be protected in the attack defense domain.

Configuring Policy Self-learning

Command	Egress gateway: net-defend learning net-defend-zone-name [days days]
Parameter Description	net-defend-zone-name: Indicates the name of the network attack defense domain. days: Indicates the number of policy learning days. The value ranges from 3 to 60 and the default value is **7**.
Command Mode	Privileged EXEC mode
Usage Guide	Policy suggestions provided via defense policy learning are policies generated for common attack problems, and not all policies can be deployed on the firewall. It is recommended to enable traffic monitoring during policy learning, to check the type of traffic that enters or leaves the network attack defense domain. This information facilities the configuration of access control.

Enabling a Policy for Defending Against TCP SYN Flood Attacks

Command	Egress gateway: tcp-unauth { syns-in | half-conn-in } global threshold threshold-num [timeout seconds] action { anti-spoofing | notify }
Parameter Description	threshold-num: When **syns** is set, it indicates the maximum number of packets per second (pps) and the value ranges from 1 to 800,000. When **half-conn** is set, it indicates the maximum number of semi-connections and the value ranges from 1 to 10,000,000. seconds: Indicates the minimum execution duration of a policy, in seconds. The value ranges from 10 to 86,400.
Command Mode	Network attack defense domain configuration mode
Usage Guide	The defense mechanism is enabled when the rate of SYN packets (syns-in) that enter the network attack defense

	domain but do not pass the source verification exceeds the threshold, or when the number of incomplete TCP handshake connections (half-conn-in) exceeds the threshold. That is, the anti-forgery technology (anti-spoofing) is applied to the SYN packets that enter the network attack defense domain or only the attack event is recorded, and the execution time of the defense mechanism is not shorter than the value of *seconds*. The defense mechanism is enabled when the rate of SYN packets that are destined for any host (dst-ip) in the network attack defense domain but do not pass the source verification exceeds the threshold, or when the number of incomplete TCP handshake connections of the destination host exceeds the threshold. That is, the anti-forgery technology (SYN-cookie technology here) is applied to all SYN packets destined for the host, and the execution time of the defense mechanism is not shorter than the value of *seconds*. Multiple such policies can be configured. The SYN-cookie technology uses the TCP cookie verification technology to defend against packets from fake source IP addresses. The SYN-cookie technology can verify the authenticity of session sources in proxy mode.

Enabling a Policy for Defending Against TCP Traffic from Authentic Source IP Addresses

Command	tcp-auth { conn-in | half-conn-in | syns-in } src-ip threshold threshold-num [timeout seconds] action { limit | blocking | notify }
Parameter Description	threshold-num: When **conn-in**/**half-conn-in** is set, it indicates the maximum number of connections and the value ranges from 1 to 10,000,000. When **syns-in** is set, it indicates the maximum number of packets per second (pps) and the value ranges from 1 to 800,000. seconds: Indicates the minimum execution duration of a policy, in seconds. The value ranges from 10 to 86,400.
Command Mode	Network attack defense domain configuration mode
Usage Guide	The device starts the defense mechanism when the number of TCP concurrent connections (conn-in) initiated from any authentic source host (src-ip) to the network attack defense domain exceeds the threshold, when the number of incomplete TCP handshake semi-connections (half-conn-in) exceeds the threshold, or when the rate of initiated TCP SYN packets exceeds the threshold. The device limits the number of concurrent connections/limits the rate (according to the threshold), blocks all traffic of the source host that enters or leaves the network attack defense domain (according to the policy execution time), or only records the attack event. The policy execution duration is not shorter than the value of *seconds*. Multiple such policies can be configured. When this policy is configured, if the number of concurrent streams exceeds the value of **threshold-num**, the streams that fall outside the threshold will be stopped.

Enabling a Policy for Defending Against UDP, ICMP, and Other Protocol Traffic That Does Not Pass Authentic Source Verification

Command	Egress gateway: { udp | icmp | other-protocol } unauth-src-in global threshold threshold-num [timeout seconds] action { limit | drop | notify }
Parameter Description	threshold-num: Indicates the maximum number of packets per second. The value ranges from 1 to 100,000,000. seconds: Indicates the minimum execution duration of a policy, in seconds. The value ranges from 10 to 86,400.
Command Mode	Network attack defense domain configuration mode
Usage Guide	When the rate of UDP, ICMP, or other protocol packets that enter the network attack defense domain but do not pass the source verification exceeds the threshold, the device starts the defense mechanism. The device limits the

	rate (not exceeding the threshold) of the packets entering the network attack defense domain, discards all such packets, or only records the attack event. When the rate of UDP, ICMP, or other protocol packets that are destined for any host in the network attack defense domain but do not pass the source verification exceeds the threshold, the device starts the defense mechanism. The device limits the rate (not exceeding the threshold) of the packets entering the host or discards all such packets. Multiple such policies can be configured. When this policy is configured, if the number of concurrent streams exceeds the value of **threshold-num**, the streams that fall outside the threshold will be stopped.

Enabling a Policy for Defending Against UDP, ICMP, and Other Protocol Traffic from Authentic Source Hosts

Command	{ udp | icmp | other-protocol } auth-src-in src-ip threshold threshold-num [timeout seconds] action { limit | blocking | notify }
Parameter Description	threshold-num: Indicates the maximum number of packets per second. The value ranges from 1 to 100,000,000. seconds: Indicates the minimum execution duration of a policy, in seconds. The value ranges from 10 to 86,400.
Command Mode	Network attack defense domain configuration mode
Usage Guide	When the rate of UDP, ICMP, or other protocol traffic that is from any authentic source host and enters the network attack defense domain exceeds the threshold, the device starts the defense mechanism. The device limits the rate (not exceeding the threshold) of such packets that are from the source host and enter the network attack defense domain, blocks all traffic of the source host that enters or leaves the network attack defense domain (according to the policy execution time), or only records the attack event. The policy execution duration is not shorter than the value of *seconds*. Multiple such policies can be configured.

Limiting the UDP, ICMP, and Other Protocol Traffic That Enters Network Attack Defense Domain

Command	Egress gateway: { udp | icmp| other-protocol } pkt-in global threshold threshold-num [timeout seconds] action { limit | notify }
Parameter Description	threshold-num: Indicates the maximum number of packets per second. The value ranges from 1 to 100,000,000. seconds: Indicates the minimum execution duration of a policy, in seconds. The value ranges from 10 to 86,400.
Command Mode	Network attack defense domain configuration mode
Usage Guide	When the rate of UDP, ICMP, or other protocol traffic that enters the network attack defense domain exceeds the threshold, the device limits the rate of the traffic to be lower than or equal to the threshold or only records the attack event. The policy execution duration is not shorter than the value of *seconds*. When the rate of UDP, ICMP, or other protocol traffic destined for any host in the network attack defense domain exceeds the threshold, the device limits the rate of such traffic destined for the host to be lower than or equal to the threshold. The policy execution duration is not shorter than the value of *seconds*. Multiple such policies can be configured.

Configuring Anti-scanning

Command	scan { in | out } src-ip threshold { low | medium | high } [timeout seconds] action { notify | blocking | notify }
Parameter Description	in: Indicates that defense is against scanning from an external network towards the network attack defense domain. out: Indicates that defense is against scanning from the network attack defense domain towards an external network.

	low/medium/high: Indicates the sensitivity for identifying a scanning behavior. seconds: Indicates the minimum execution duration of a policy, in seconds. The value ranges from 10 to 86,400.
Command Mode	Network attack defense domain configuration mode
Usage Guide	This command is used to defend against scanning behaviors towards and from the network attack defense domain. Multiple such policies can be configured. Run the **scan policy** command to adjust anti-scanning parameters. ⚠ When the sensitivity of the anti-scanning function is low, it is not recommended to enable the defense against the ICMP destination unreachable attack. The reason is that when the sensitivity of the anti-scanning function is low, the device judges whether a scanning attack occurs based on ICMP destination unreachable packets. The defense against the ICMP destination unreachable attack will filter out ICMP unreachable packets, result in anti-scanning detection misjudgment.

Limiting the Bandwidth of Traffic That Enters or Leaves the Network Attack Defense Domain

Command	Egress gateway: ratelimit { in | out } src-ip bandwidth bps-number
Parameter Description	src-ip: Limits the bandwidth of each source IP address. dst-ip: Limits the bandwidth of each destination IP address. bps-number: Indicates the bandwidth limit, in bps. The value ranges from 1 to 1,000,000,000.
Command Mode	Network attack defense domain configuration mode
Usage Guide	When both **src-ip** and **dst-ip** are not configured, the bandwidth of all traffic that enters or leaves the network attack defense domain is limited. If traffic comes from hosts whose authenticity is not confirmed, such traffic is not limited by the policy. Multiple such policies can be configured.

Limiting the Creation Rate of Sessions That Enter or Leave the Network Attack Defense Domain

Command	session-limit { in | out } [src-ip | dst-ip] session-rate new-session-per-second
Parameter Description	src-ip: Limits the session creation rate of each source IP address. dst-ip: Limits the session creation rate of each destination IP address. new-session-per-second: Indicates the limited session creation rate. The value ranges from 1 to 100,000.
Command Mode	Network attack defense domain configuration mode
Usage Guide	When both **src-ip** and **dst-ip** are not configured, the creation rate of all sessions of the network attack defense domain is limited. If a session is from a host whose authenticity is not confirmed, the session is not limited by the policy. Multiple such policies can be configured.

Configuring a Bypass Traffic Policy

Command	Egress gateway: bypass src-ip-address [mask src-ip-mask] [proto { tcp | udp | icmp | protocol-num }]
Parameter Description	src-ip-address: Indicates the source IP address. src-ip-mask: Indicates the subnet mask of the source IP address.

	protocol-num: Indicates the protocol number. dest-port-num: Indicates the destination port number.
Command Mode	Network attack defense domain configuration mode
Usage Guide	This command is used to configure bypass traffic that can enter the network attack defense domain. You can run this command to enable packets from a specified source IP address to directly enter the network attack defense domain without attack defense processing, and enable packets from the network attack defense domain to directly go to the destination IP address without attack defense processing. You can define multiple bypass traffic policies. The traffic that matches any one policy is considered as bypass traffic. The system does not automatically combine multiple overlapping bypass commands. Packets that match bypass traffic policies will bypass all attack defense processing and will not be counted by the traffic monitoring function of the attack defense. ⚠ After a packet matches a bypass traffic policy, other policies relevant to the network attack defense domain will not be applied to the packet. If a packet matches the bypass traffic policy and blacklist, the bypass policy is prior to the blacklist. ⚠ The bypass configuration is valid only to the local network attack defense domain. ⚠ The **bypass** command exempts hosts outside the network attack defense domain from defense policies and enables them to freely access the hosts in the network attack defense domain. Users should not set **src-ip-address** in the **bypass** command to the IP address of a host in the network attack defense domain. ⚠ The bypass traffic policy does not support automatic association of parent and child flows. That is, if users need to configure a bypass traffic policy for accessing the FTP service of the network attack defense domain, it is not recommended to configure the destination port ID, so as to prevent a bypass traffic failure in data channels.

Configuring a Blacklist

Command	blacklist ip-address
Parameter Description	ip-address: Indicates the host IP address.
Command Mode	Network attack defense domain configuration mode
Usage Guide	This command is used to add a host to the blacklist to forbid the traffic of the host from entering or leaving the network attack defense domain. Multiple blacklists can be configured. ⚠ Different from the bypass traffic policy, the blacklist function allows users to blacklist hosts inside and outside the network attack defense domain. Once a host is blacklisted, the traffic of the host is forbidden to pass through the firewall.

Configuring Traffic Monitoring

Command	traffic-monitor { tcp | http | udp | icmp | ip | all }
Parameter Description	N/A
Command	Network attack defense domain configuration mode

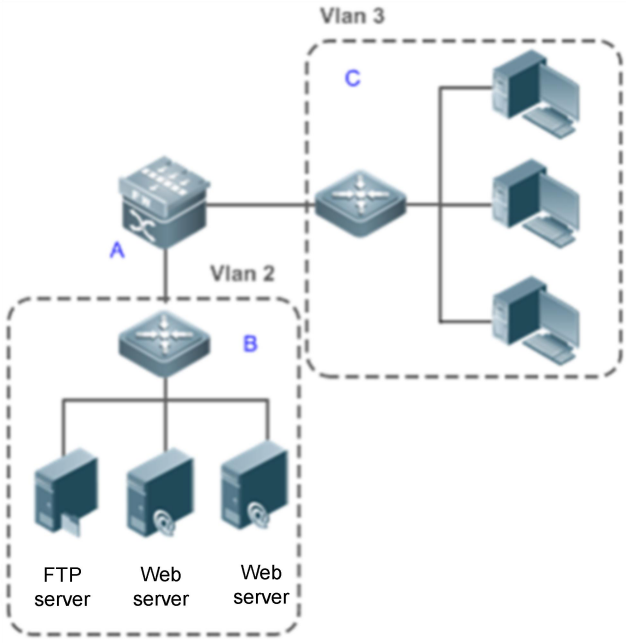
Mode	
Usage Guide	This command is used to enable monitoring on various types of traffic, including TCP, HTTP, UDP, ICMP, and IP traffic. Traffic monitoring can be simultaneously deployed with policy self-learning and defense policies.

Configuring the Log Function

Command	log { tcp-auth | tcp-unauth | icmp | udp | other-protocol | scan | all } [syslog | save]
Parameter Description	N/A
Command Mode	Network attack defense domain configuration mode
Usage Guide	The log function allows users to enable the log and printing functions for a specified policy type. Multiple such policies can be configured. When **syslog** or **save** is not carried in the command, attack information is both recorded in the system logs and database. ⚠ When the policy threshold is not set appropriately or a large number of attacks occur in an instant, a large number of logs will be generated in a short period of time and some of history logs may be lost.

Configuration Example

Creating a Network Attack Defense Domain Named web and Enabling Policy Self-learning and Traffic Monitoring for the Domain

Scenario **Figure 26- 6**	
Configuration Steps	● On the egress gateway, create a network attack defense domain named web and associate it with an ACL. In a NAT scenario, the ACL needs to contain the NAT internal and external IP addresses of the protected area. ● Configure traffic monitoring for the network attack defense domain. ● Enable policy self-learning for the network attack defense domain.
A	A# configure terminal

	Enter configuration commands, one per line. End with CNTL/Z. A(config)#ip access-list standard servers A(config-std-nacl)# permit 192.168.1.0 0.0.0.255 A(config-std-nacl)# exit A(config)# defend-zone web A(config-defend-zone)# description “Web server zone” A(config-defend-zone)# ip access-group servers A(config-defend-zone)# traffic-monitor all A(config-defend-zone)# exit A(config)# exit A# net-defend learning web
Verification	● Check the status of the network attack defense domain named web. ● Enable a host in the external network to send various types of traffic to any server in the network attack defense domain. ● Check the traffic snapshots. ● Wait 7 days. The policy learning ends (if the function needs to be verified, reduce the time to 1 day). ● Check the policy learning results.
A	A# show defend-zone web Description: Web server zone Zone state: Learning (End time: 2013-03-12 11:24:17) ACL associated: servers Traffic monitor: tcp, http, udp, icmp, ip A# show defend-zone web traffic-snapshot Total Pkts current bps Received 1234567891 12567893 Dropped 0 0 Replied 12114 1983 TCP FLOW: Syns in: 672 pps Connections(in): 987374 Half-connections (in): 23453 Bandwidth (in): 573823453 bps Bandwidth (out): 829353321 bps HTTP FLOW: Syns in:1200 pps Connections(in): 987374 UDP FLOW: Pkts (in):289 pps Pkts (out):289 pps

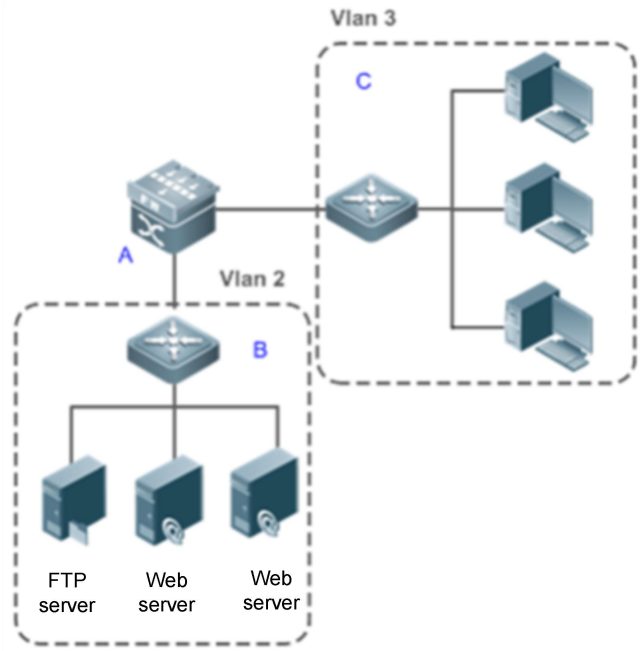
```
      Bandwidth (in): 57382 bps
      Bandwidth (out): 8293 bps

    ICMP FLOW:
      Pkts (in):289 pps
      Pkts (out):289 pps
      Bandwidth (in): 57382 bps
      Bandwidth (out): 8293 bps

    IP FLOW:
      Pkts (in):289 pps
      Pkts (out):289 pps
      Bandwidth (in): 57382 bps
      Bandwidth (out): 8293 bps

A# show net-defend learning    web
Learning status:Learning (End time:2013-03-12 11:24:17)
<TCP flow statistic (in)>
      Every auth-src-ip:
            Max half connection:20
            Max connection: 500
            Max syns (pps): 50
      Global:
            Max half connection: 293829
            Max syns (pps): 1453
<UDP flow statistic (in)>
      Unauth-src UDP flow rate(pps):    2000
      Every auth-src-ip:
            Max UDP flow rate(pps): 1020
      Global:
            Max UDP flow rate(pps): 60345
<ICMP flow statistic (in)>
      Unauth-src ICMP flow rate(pps):    10
      For every auth-src-ip:
            Max ICMP flow rate(pps): 3
<Other-protocol flow statistic (in)>
      Unauth-src Other-protocol flow rate(pps):    0
      For every auth-src-ip:
            Max Other-protocol flow rate(pps): 0

Advices net defend polices for defend-zone 'web':
! These policies for anti-spoofing (TCP SYN Flooding Attack)
tcp-unauth half-conn-in global threshold    293829 action anti-spoofing
tcp-unauth syns-in global threshold    1453 action anti-spoofing
```

```
! These policies for Client Attack
tcp-auth conn-in src-ip threshold 1000 action notify
tcp-auth half-conn-in src-ip threshold 20 action notify
tcp-auth syns-in src-ip threshold 50 action notify

! These policies for UDP/ICMP/Other-protocol Flooding Attack
udp unauth-src-in global threshold    2000 notify
udp auth-src-in src-ip threshold    1000 notify
udp pkt-in global threshold 60345 action notify
icmp unauth-src-in global threshold 10 timeout 600 notify
icmp auth-src-in src-ip threshold 3 timeout 600 notify
other-protocol unauth-src-in global threshold 10 timeout 600 notify
other-protocol auth-src src-ip threshold 5 timeout 600 notify
```

Creating a Network Attack Defense Domain Named web, and Configuring Defense Policies and the Log Function

Scenario

Figure 26- 7



Configuration Steps

- On the egress gateway, create a network attack defense domain named web and associate it with an ACL.
- Configure defense policies for the network attack defense domain.
- Configure the log function for the network attack defense domain.

A

```
A# configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
A(config)#ip access-list standard servers
A(config-std-nacl)# permit 192.168.1.0 0.0.0.255
A(config-std-nacl)# exit
A(config)# defend-zone web
A(config-defend-zone)# description "Web server zone"
A(config-defend-zone)# ip access-group servers
```

	A(config-defend-zone)# tcp-unauth half-conn-in global threshold 30000 action anti-spoofing A(config-defend-zone)# udp unauth-src-in global threshold 10000 notify A(config-defend-zone)# log all A(config-defend-zone)# exit
Verification	● Check the status of the network attack defense domain named web. ● Enable a host in the external network to send TCP SYN and UDP traffic with fake source IP addresses to a server in the network attack defense domain. ● Check the underway attack (you can enable the debug function to receive attack event notifications). ● Stop the attack and check the attack report.
A	A# show defend-zone web Description: Web server zone Zone state: Running ACL associated: servers A# show defend-zone web running-protect Defend zone: 'web', Total report: 2 Attack type: 'TCP SYN Flood' id: 823 Begin:2013-3-5 12:03:04 ,timeout 60s Flow: * -> *, Action: Anti-spoofing(syn cookie) Policy: tcp-unauth:half-conn:global Threshold:30000, current: 30000 Received:2334354, Replied: 1453467, Dropped:0 Attack type: 'UDP Flood (Spoofed)' id: 824 Begin:2013-3-5 12:21:53 ,timeout 60s Flow: * -> *, Action: notify Policy: udp: unauth-src-in:global Threshold:10000, current: 15235 Received:567749, Replied: 0, Dropped: 0 After the attack ends, check the attack report. A# show defend-zone web report 2013-3-5 Defend zone:'web', Total report: 2 Attack type: 'TCP SYN Flood' 2013-3-5 12:03:04 ~ 2013-3-5 13:10:23 Flow: * -> *, Action: Anti-spoofing(syn cookie) Policy: tcp-unauth:half-conn:global Threshold: 30000, Action: Anti-spoofing(syn cookie) Received: 6343364, Replied: 4362364, Dropped: 0 Attack type: 'UDP Flood (Spoofed)'

	2013-3-5 12:21:53 ~ 2013-3-5 13:08:113 Flow: * -> *, Action: notify Policy: tcp-unauth:half-conn:global Threshold: 10000, Action: notify Received: 4345239, Replied: 0, Dropped: 0

Common Errors

- An unsupported ACL is associated.
- When NAT is enabled on the egress gateway, the ACL associated with the network segments protected by the attack defense domain contains only NAT internal IP addresses of the network segments, or incomplete external IP address segments, or incomplete internal IP address segments corresponding to the contained external IP address segments.
- An excessively large network attack defense domain is created. For example, the Internet is configured as a network attack defense domain. This will cause excessive resource consumption.
- When dual firewall service modules are inserted into the core switch, the values of the restriction parameters in all policies of the network attack defense domain are reduced by half on each service module. For example, the rate of packets destined for each host in the network attack defense domain is configured to be no more than 1,000,000 bps. Then, the rate of packets destined for each host in the network attack defense domain does not exceed 500,000 bps on each firewall service module.

26.1.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears statistics of the network attack defense domain.	Egress gateway: clear defend-zone net-defend-zone-name counters

Displaying

Description	Command
Displays the status of the attack defense service module.	show defend module
Displays the status of the network attack defense domain.	Egress gateway: show defend-zone net-defend-zone-name [counters | host]
Displays packet loss statistics of the network attack defense function.	Egress gateway: show defend drop
Displays the current traffic snapshots.	Egress gateway: show defend-zone net-defend-zone-name traffic-snapshot { tcp [syns-in | conn-in | half-conn-in | bandwidth] [topn] | http [syns-in | conn-in] | { ip | udp | icmp } [bandwidth | pkts] }
Displays underway attacks by policy type.	Egress gateway: show defend-zone net-defend-zone-name running-protect [tcp-auth | tcp-unauth | icmp | udp | other-protocol | scan | protect-id]

Displays underway attacks by attack type.	Egress gateway: show defend-zone net-defend-zone-name running-protect attack { tcp-syn-flood | tcp-conn-flood | udp-spoof-flood | icmp-spoof-flood | other-spoof-flood | udp-flood | icmp-flood | other-flood | scan }
Displays completed protection by time.	Egress gateway: show defend-zone net-defend-zone-name report [begin-date [begin-hour] [to end-date [end-hour]]] [tcp-auth | tcp-unauth | icmp | udp | other-protocol | scan | attack { tcp-syn-flood | tcp-conn-flood | udp-spoof-flood | icmp-spoof-flood | other-spoof-flood | udp-flood | icmp-flood | other-flood | scan }]
Displays current anti-scanning configuration parameters.	show scan parameter

Fixing

Description	Command
Synchronizes the configuration of the current device to the service module of the firewall.	Egress gateway: sync defend config [net-defend-zone-name] [force] When the **show defend-zone net-defend-zone-name** command shows that the status of the network attack defense domain is "FWM error", the network attack defense domain is not configured to the service module of the firewall. In this case, run this command to synchronize the configuration.

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs attack defense data integrity.	debug netdefend data
Debugs the information exchange between the anti-attack Supervisor Engine and firewall service module.	debug netdefend rpc

26.2 Configuring the Security Zone

26.2.1 Overview

A security zone is a logical area composed of a group of systems that have the same security protection requirements and trust each other. It is classified in the same logical area by nature of information, application object, security objective, policy, and other elements. All systems in the logical area have the same security protection requirements as well as the same security access control and boundary control policies. Security zones aim to transform security problems of a large-scale complex system into security protection problems of smaller zones. Currently, security zones are primarily used for access control. With security zones, administrators can assign interfaces or IP addresses with the same security requirements (into different zones) to implement hierarchical management of policies. For example, four interfaces connected to different network segments of the terminal zone can be added to the security zone "TERM", and two interfaces connected to the server zone can be added to the security zone "Server". In this way, administrators need to only deploy security policies between the two zones. In a word, security zones simplify policy maintenance.

Protocols and Standards

N/A

26.2.2 Applications

Application	Description
Controlling Access Permissions by Using Security Zone Access Policies	An access policy is configured for a security zone to control access permissions.

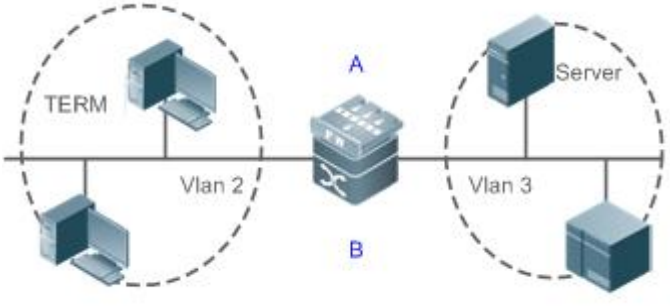
26.2.2.1 Controlling Access Permissions by Using Security Zone Access Policies

Scenario

A security zone access policy is configured on an enterprise network to control access permissions.

As shown in the figure below, the firewall module controls the access to the two zones (TERM zone and Server zone).

Figure 266- 8



Deployment

- Add two security zones: TERM and Server.
- Configure a security zone access policy: Hosts in the TERM security zone can access only specific services of the Server security zone.

26.2.3 Features

Basic Concepts

Security Zone Division Method

Security zones can be divided in two ways: by IP address set and by network interface. The two methods are exclusive. Security zones are divided by interface by default. Only IPv4 address sets are supported when security zones are divided by IP address set. IPv6 address sets are not supported.

Security Zone Priority

A priority can be configured for each security zone to control default mutual access between security zones. Hosts in a higher-priority security zone are allowed to access a lower-priority security zone but hosts in the lower-priority security zone are not allowed to access the higher-priority security zone. Access is not allowed between security zones with the same priority by default.

Intra–Security Zone Policy

An intra–security zone policy is used for access control within the same security zone. By default, hosts in a security zone cannot access each other unless the security zone is configured to support mutual access or a global access policy is configured to support intra–security zone access.

Inter–Security Zone Policy

An inter–security zone policy is used to control the access across security zones. You can configure security zone–based policies to implement the mutual access control between security zones. An inter–security zone policy maintains an ACL between the source security zone and destination security zone. A string of matching rules can be configured in the ACL to identify specific packets and allow or reject the packets to pass according to preset conditions. Apart from ACL-based policies, inter–security zone access policies can be configured in two ways (known as default mutual access control rules):

- Configuring security zone priorities to control the mutual access between security zones
- Configuring a global access policy to control the mutual access between security zones with the same priority

⚠ Inter–security zone policies are prior to default mutual access control rules, which work only when no inter–security zone policy exists.

Global Access Policy for Security Zones

A global access policy globally controls whether mutual access is allowed in a security zone and between security zones with the same priority. The policy also controls whether logs are generated in the case of connection release when a security zone policy is matched and in the case of packet discarding due to violation of a security zone access policy.

⚠ The communication with the local device (including packets sent or received by the local host) is not affected by security zone policies.

Overview

Feature	Description
Dividing Security Zones by IP Address Set	Determine the security zone division method.
Dividing Security Zones by Network Interface	Determine the security zone division method.
Security Zone Access Policy	Configure policies for access from one security zone to another.
Global Access Policy for Security Zones	Configure a global access control policy.

26.2.3.1 Dividing Security Zones by IP Address Set

Administrators can set the corresponding relationship between security zones and information system sets according to requirements of specific applications:

- A security zone uses a security zone name as the unique identifier.
- The information system is identified by IP address, and an information system set is a set of IP addresses.

After the corresponding relationship between security zones and information systems is defined, IP addresses that cannot match the information system corresponding to the security zones are allocated to the default security zone. The default security zone is a special security zone, which exists by default but cannot be deleted.

Working Principle

After packets arrive at the firewall module, the firewall module identifies the source and destination IP addresses of the packets and matches the IP addresses with the ACLs associated with security zones, to determine the source and destination security zones of the packets.

Related Configuration

Dividing Security Zones by IP Address Set

By default, security zones are divided by network interface.

Run the **no security-zone-base interface** command to switch to security zone division based on IP address set.

Switching the security zone division method will delete all existing security zones, security zone access policies, and global access policies.

Configuring an ACL Associated with a Security Zone

By default, no ACL is associated with a security zone and in this case, the security zone does not work because of incomplete configuration. The default security zone cannot associate with an ACL. If a packet cannot match any created security zone, it is allocated to the default security zone.

26.2.3.2 Dividing Security Zones by Network Interface

Administrators can set the corresponding relationship between security zones and network interfaces according to requirements of specific applications:

- A security zone uses a security zone name as the unique identifier.
- Set the security zone, to which a network interface belongs.

Interfaces, for which no security zone is configured, are allocated to the default security zone. The default security zone is a special security zone, which exists by default but cannot be deleted.

Working Principle

After packets arrive at the firewall module, the firewall module identifies the source and destination interfaces of the packets and matches the interfaces with network interfaces associated with security zones, to determine the source and destination security zones of the packets.

Related Configuration

Dividing Security Zones by Network Interface

By default, security zones are divided by network interface.

If security zones are divided by IP address set, run the **no security-zone-base interface** command to switch to security zone division based on network interfaces.

Switching the security zone division method will delete all existing security zones, security zone access policies, and global access policies.

Adding an Interface to a Security Zone

By default, no interface is added to a security zone. In this case, the security zone does not work because no packet will match the security zone. No interface can be added to the default security zone. If a packet cannot match any created security zone, it is allocated to the default security zone.

In security zone configuration mode, run the **interface** command to add an interface to a security zone.

26.2.3.3 Security Zone Access Policy

Working Principle

After packets arrive at the firewall module, the firewall module, based on packet characteristics, identifies the source and destination security zones of the packets. If the source security zone is not the same as the destination security zone, inter–security zone access is involved. In this case, the firewall module first searches for an inter–security zone access policy. If no such policy is found, it compares the priority of the source security zone with that of the destination security zone. If the former is higher than the latter, access is allowed. If the former is lower than the latter, access is rejected. If the priorities are the same, the firewall module determines whether to allow access between security zones with the same priority according to the global function configuration. If the source security zone is the same as the destination security zone, intra–security zone access is involved. The firewall module first checks whether there is an intra–security zone access policy. If no such policy is found, the firewall module checks whether intra–security zone access is enabled in the security zone. If no relevant policy is found, the firewall module determines whether to allow intra–security zone access according to the global function configuration.

Security zones divided by network interface support ACL-based and object-based security zone access policies. If an ACL-based policy is adopted, the firewall module extracts addresses and port information from IP packets and matches them with the ACL in the policy. If they match, the firewall module determines whether to allow or reject the packets to pass based on the ACE attribute (permit or deny) in the ACL. If an object-based policy is adopted, the firewall module extracts addresses and port information from IP packets, matches the addresses with address objects in the policy, and matches port IDs with service objects in the policy. If the packets match the policy, the firewall module determines whether to allow or reject the packets to pass based on the rule attribute (permit or deny).

⚠ An ACL-based access policy cannot coexist with an object-based access policy and they are controlled by the **security-access-match-object** command. The ACL-based access policy is enabled by default. Currently, object-based access policies support only IPv4 packets and not IPv6 packets.

Related Configuration

Using Object-based Security Zone Access Policies for Packet Matching

By default, ACL-based security zone access policies are used for packet matching.

Run the **security-access-match-object** command to use object-based security zone access policies for packet matching.

Configuring an ACL-based Policy for IPv4 Packet Access from One Security Zone to Another

By default, there is no policy for IPv4 packet access from one security zone to another.

Run the **security-access** command to add a policy for IPv4 packet access from one security zone to another.

When the source security zone is the same as the destination security zone in a rule, the rule is an intra–security zone policy.

Configuring an Object-based Policy for IPv4 Packet Access from One Security Zone to Another

By default, there is no policy for IPv4 packet access from one security zone to another.

Run the **security-access** command to add a policy for IPv4 packet access from one security zone to another.

When the source security zone is the same as the destination security zone in a rule, the rule is an intra–security zone policy.

Configuring the Default Sequence Number Step for Security Zone Access Policies

By default, the sequence numbers of security zone access policies increase at a step of 10.

Run the **security-access-step** command to change the default sequence number step for security zone access policies.

26.2.3.4 Global Access Policy for Security Zones

Global access policies globally control the access within a security zone and between security zones.

Working Principle

See the description in the preceding section. Global access policies also control whether logs are generated in the case of a connection establishment after a security zone policy is met or in the case of packet discarding because a security zone policy is not met.

Related Configuration

Allowing Mutual Access Within a Security Zone

By default, mutual access within a security zone is not allowed if the intra–security zone access policy is not matched.

Run the **loose-inner-zone-access** command to enable mutual access within a security zone when the intra–security zone access policy is not matched.

Allowing Mutual Access Between Security Zones with the Same Priority

By default, mutual access is no allowed between security zones with the same priority if the inter–security zone access policy is not matched.

Run the **loose-inter-zone-access** command to allow mutual access between security zones with the same priority when an inter-security zone access policy is not matched.

Configuring Log Generation in the Case of Connection Release After a Security Zone Policy Is Matched

By default, logs are not generated in the case of connection release after a security zone policy is met.

Run the **security-permit-access-log** command to configure log generation in the case of connection establishment and release after a security zone policy is matched.

Configuring Log Generation in the Case of Packet Discarding due to Violation of a Security Zone Access Policy

By default, logs are not generated in the case of packet discarding due to violation of a security zone access policy.

Run the **security-deny-access-log** command to configure log generation in the case of packet discarding due to violation of a security zone access policy.

Currently, logs are output in the form of system logs. Enabling the log function will degrade the device performance. The log function is used for troubleshooting only and is recommended to be disabled under normal circumstances.

26.2.4 Configuration

Configuration	Description and Command	
Configuring a Security Zone	(Mandatory) It is used to create a security zone.	
	security-zone-base	Configures the security zone division method.
	security-zone	Creates a security zone or enters an existing security zone.
	description	Configures a description string for the security zone.
	security-level	Configures the priority for the security zone.
	inner-zone-access	Allows IP mutual access within the security zone when the access policy of the security zone is not matched.
	interface	Adds an interface to the security zone.
Configuring a Security Zone Access Policy	(Optional) It is used to configure a security zone access policy.	
	security-access-match-object	Uses object-based security zone access policies for packet matching.
	security-access	Configures a policy for IPv4 packet access from one security zone to another.
	security-access-step	Configures the default sequence number step for security zone access policies.
Configuring a Global Access Policy for Security Zones	(Optional) It is used to configure a global access policy.	
	loose-inner-zone-access	Globally allows IP mutual access within a security zone when the intra–security zone access policy is not matched.
	loose-inter-zone-access	Globally allows mutual access between security zones with the same priority when the inter–security zone access policy is not matched.
	security-permit-access-log	Configures log generation in the case of connection release after packet traffic matches a security zone policy.
	security-deny-access-log	Configures log generation in the case of packet discarding due to violation of a security zone access policy.

26.2.4.1 Configuring a Security Zone

Configuration Effect

Determine the security zone division method and create a security zone.

Notes

Determine the security zone division method and then configure security zones. Switching the security zone division method will delete all existing security zones, security zone access policies, and global access policies.

Configuration Steps

Configuring the Security Zone Division Method

- (Optional) Security zones are divided by interface by default.
- Perform the configuration in privileged EXEC mode.

Creating a Security Zone or Going to an Existing Security Zone

- (Optional) A security zone named default exists by default. New security zones also need to be created.
- Perform the configuration in privileged EXEC mode.

Configuring the Priority for the Security Zone

- (Optional) Configure the priority when the access between security zones needs to be controlled based on the security zone priority.
- Perform the configuration in security zone configuration mode.

Allowing IP Mutual Access Within the Security Zone When the Access Policy of the Security Zone Is Not Matched

- (Optional) Complete the configuration when the mutual access in a security zone needs to be controlled.
- Perform the configuration in security zone configuration mode.

Configuring a Description String for the Security Zone

- Optional.
- Perform the configuration in security zone configuration mode. You are recommended to configure it for better memorization.

Configuring an ACL Associated with the Security Zone

- Mandatory for security zones divided or created based on IP address sets.
- Perform the configuration in security zone configuration mode.

Adding an Interface to the Security Zone

- Mandatory for security zones divided or created based on network interfaces.
- Perform the configuration in security zone configuration mode.

Verification

Use the security zone priority for access control and check whether the access control between hosts in different security zones is in line with the security zone priority.

Related Commands

Configuring the Security Zone Division Method

Command	security-zone-base interface
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	When the security zone division method is changed, all existing security zones, security zone access policies, and global access policies will be cleared. When security zones are divided by IP address set, the security zone policy is applied only to IPv4 packets and IPv6 packets are allowed to pass directly.

Creating a Security Zone or Going to an Existing Security Zone

Command	security-zone *zone-name*
Parameter Description	*zone-name*: Indicates the name of a security zone. The value is a string of 1–32 characters. A security zone named default is retained in the system, and can be neither created nor deleted.
Command Mode	Privileged EXEC mode
Usage Guide	A security zone named default exists by default. You can run the **security-zone default** command to enter the configuration mode of this security zone. This security zone can be neither created nor deleted.

Configuring a Description String for the Security Zone

Command	description *string*
Parameter Description	*string*: Indicates the description string of the security zone. The value is a string of 1–40 characters.
Command Mode	Security zone mode
Usage Guide	N/A

Configuring the Priority for the Security Zone

Command	security-level *level-num*
Parameter Description	*level-num*: Indicates the priority of the security zone. The value ranges from 1 to 100. A larger value indicates a higher priority.
Command Mode	Security zone mode
Usage Guide	By default, a security zone has no priority for comparison.

Allowing IP Mutual Access Within the Security Zone When the Access Policy of the Security Zone Is Not Matched

Command	inner-zone-access
Parameter Description	N/A

Command Mode	Security zone mode
Usage Guide	By default, IP mutual access is not allowed within a security zone if the access policy of the security zone is not matched. The priority of this command is higher than that of the global **loose-inner-zone-access** command. If this command is not configured, the configuration of the global **loose-inner-zone-access** command shall prevail.

Adding an Interface to the Security Zone

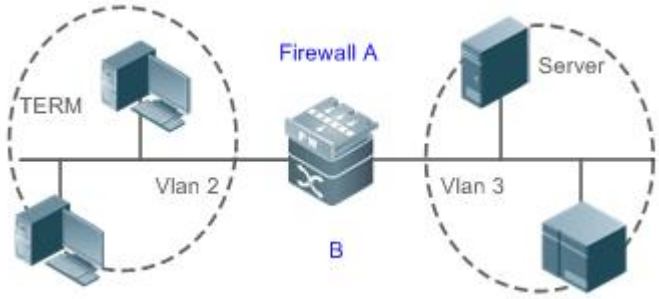
Command	**interface** *interface-name*
Parameter Description	*interface-name*: Indicates the interface name.
Command Mode	Security zone mode
Usage Guide	Multiple interface names can be configured for one security zone but one interface can belong to only one security zone. ⚠ This configuration is applicable only to security zones divided by network interface. ⚠ The default security zone does not support the **interface** command. ⚠ On the virtual firewall in non-routing mode, only VLAN interfaces can be added to security zones. On the virtual firewall in routing mode (route-mode-vfw), layer-3 physical interfaces, layer-3 APs, and SVIs can be added to security zones.

Checking the Configuration of a Single or All Security Zones

Command	**show security-zone** [*zone-name*]
Parameter Description	*zone-name*: Indicates the name of a security zone. By default, the configuration of all security zones is displayed.
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	This command is used to display the configuration of a single or all security zones. Security zone information includes the description string, priority, associated access-group or contained interfaces, and whether mutual access is allowed within the security zone.

Configuration Example

Configuring the Interface-based Security Zone Division Method, Using the Security Zone Priority for Access Control, and Allowing Hosts in the TERM Zone to Access the Server Zone but Rejecting Hosts in the Server Zone to Access the TERM Zone

Scenario	
Figure 266- 9	
Configuration	● Configure the firewall to protect data flowing in and out of VLAN 3 and configure VLAN 103 as a traffic

Steps	diversion VLAN. For details about traffic diversion VLAN, see sections relevant to firewall management. ● Configure security zones divided by network interface. Create two security zones named TERM and Server respectively and set the priority of the TERM security zone to be higher than that of the Server security zone.
B	B(config-vfw)#security-zone TERM B(config-vfw-security-zone)#description terminal_client_zone B(config-vfw-security-zone)#security-level 80 B(config-vfw-security-zone)#interface vlan 103 B(config-vfw-security-zone)#exit B(config-vfw)#security-zone Server B(config-vfw-security-zone)#description server_zone B(config-vfw-security-zone)#security-level 10 B(config-vfw-security-zone)#interface vlan 3 B(config-vfw-security-zone)#exit
Verification	Check whether hosts in the TERM security zone can access the Server security zone while hosts in the Server security zone cannot access the TERM security zone.
B	B#show security-zone TERM security-zone:TERM description:terminal_client_zone level: 80 inner-zone access:off interface member:vlan 103 B#show security-zone Server security-zone:Server description: server_zone level: 10 inner-zone access:off interface member:vlan 3

Common Errors

- No priority is set for a security zone. By default, a security zone has no priority for comparison.

26.2.4.2 Configuring a Security Zone Access Policy

Configuration Effect

Configure a security zone access policy to control the access between different security zones.

Notes

N/A

Configuration Steps

Using Object-based Security Zone Access Policies for Packet Matching

- (Optional) The configuration is required when object-based security zone access policies need to be used for packet matching.
- Perform the configuration in privileged EXEC mode.

Configuring an ACL-based Policy for IPv4 Packet Access from One Security Zone to Another

- (Optional) The configuration is required when one ACL-associated rule needs to be used to control the access from one security zone to another.
- Perform the configuration in privileged EXEC mode.

Configuring an Object-based Policy for IPv4 Packet Access from One Security Zone to Another

- (Optional) The configuration is required when one object-associated rule needs to be used to control the access from one security zone to another.
- Perform the configuration in privileged EXEC mode.

Configuring the Default Sequence Number Step for Security Zone Access Policies

- (Optional) The configuration is required when the default sequence number step needs to be changed for security zone access policies.
- Perform the configuration in privileged EXEC mode.

Verification

Use a security zone access policy for access control and check whether the control over the access from different hosts in the same security zone to other security zones is in line with the security zone access policy.

Related Commands

Using Object-based Security Zone Access Policies for Packet Matching

Command	**security-access-match-object**
Parameter Description	*N/A*
Command Mode	Privileged EXEC mode
Usage Guide	After the **security-access-match-object** command is configured, existing ACL-based security zone access policies will be deleted. Likewise, after the **no security-access-match-object** command is configured, existing object-based security zone access policies will be deleted. ⚠ This command takes effect only when the interface-based security zone division method is adopted. ⚠ Currently, object-based access policies support only IPv4 packets and not IPv6 packets.

Configuring an ACL-based Policy for IPv4 Packet Access from One Security Zone to Another

Command	**security-access** [**sequence** *sequence-number*] **from** *zone-name* **to** *zone-name access-list* [**inactive**] [**description** *string*]
Parameter Description	*access-list*: Indicates the associated IPv4 ACL. *zone-name*: Indicates the name of a security zone. *sequence-number*: Indicates the sequence number. The value ranges from 1 to 2,147,483,647. A policy with a smaller

	sequence number is used for matching preferentially. If no sequence number is contained in this command, the system assigns a default sequence number to the entry. The default sequence number of the first entry is step-number. The default sequence number of each subsequent unassigned entry is greater than the last policy sequence number by step-number (see the **security-access-step** command). **inactive**: Indicates that a rule is not activated. *string*: Indicates the description string. The value is a string of 1–31 characters.
Command Mode	Privileged EXEC mode
Usage Guide	The name of the source security zone can be the same as that of the destination security zone. In this case, the rule is an intra–security zone access policy.

Configuring an Object-based Policy for IPv4 Packet Access from One Security Zone to Another

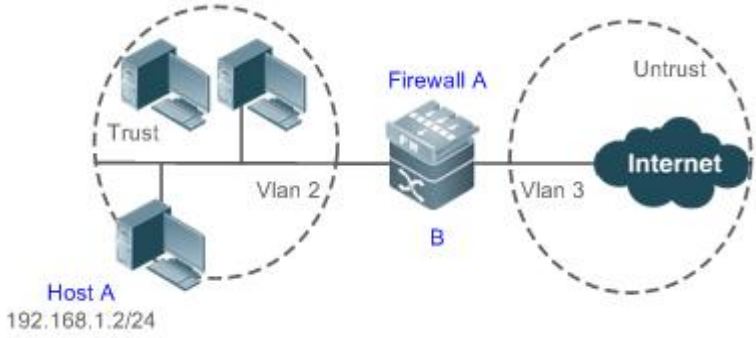
Command	**security-access** [**sequence** *sequence-number*] **from** *zone-name* to *zone-name* { **deny** | **permit** } **src-address-object** *src-object-name* **dest-address-object** *dest-object-name* **service** *serv-name* [**time-range** *time-range-name*] [**inactive**] [**description** *string*]
Parameter Description	*access-list*: Indicates the associated IPv4 ACL. *zone-name*: Indicates the name of a security zone. *sequence-number*: Indicates the sequence number. The value ranges from 1 to 2,147,483,647. A policy with a smaller sequence number is used for matching preferentially. If no sequence number is contained in this command, the system assigns a default sequence number to the entry. The default sequence number of the first entry is step-number. The default sequence number of each subsequent unassigned entry is greater than the last policy sequence number by step-number (see the **security-access-step** command). **deny**: Indicates that packets matching the rule are not allowed to pass. **permit**: Indicates that packets matching the rule are allowed to pass. *src-object-name*: Indicates the source address object, and any_address is a special address object. *dest-object-name*: Indicates the destination address object, and any_address is a special address object. *serv-name*: Indicates the service object, and any_service is a special service object. *time-range-name*: Indicates the time range associated with a rule. *string*: Indicates the description string. The value is a string of 1–31 characters. **inactive**: Indicates that a rule is not activated.
Command Mode	Privileged EXEC mode
Usage Guide	The name of the source security zone can be the same as that of the destination security zone. In this case, the rule is an intra–security zone access policy.

Configuring the Default Sequence Number Step for Security Zone Access Policies

Command	**security-access-step** *step-number*
Parameter Description	*step-number*: Indicates the default sequence number step for the **security-access** commands.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Example

- Configuring Interface-based Security Zone Division Method, Connecting the Internal Network to the Internet via Firewall, and Configuring the Internal Network to Belong to the Trust Security Zone and the External Network to Belong to the Untrust Security Zone (Only Host A in the internal network can access the Internet and other hosts cannot.)

Scenario Figure 266- 10	
Configuration Steps	● Configure the firewall to protect data flowing in and out of VLAN 3 and configure VLAN 103 as a traffic diversion VLAN. ● Configure security zones divided by network interface and create two security zones: Trust and Untrust. Associate Host A in the Trust security zone with a security zone access policy, which allows Host A to access the Untrust security zone. Do not associate other hosts with an ACL, and reject the access of other hosts to the Untrust security zone.
B	B(config-vfw)#security-zone Trust B(config-vfw-security-zone)#description trust_zone B(config-vfw-security-zone)#interface vlan 103 B(config-vfw-security-zone)#exit B(config-vfw)#security-zone Untrust B(config-vfw-security-zone)#description internet_zone B(config-vfw-security-zone)#interface vlan 3 B(config-vfw-security-zone)#exit B(config-vfw)#security-access 100 from Trust to Untrust
Verification	Check whether Host A in the Trust security zone can access the Internet but other hosts cannot access the Internet.
B	B#show security-zone Trust security-zone:Trust description:trust_zone level not defined inner-zone access:off interface member:vlan 103 B#show security-zone Untrust security-zone:Untrust description: internet_zone level not defined inner-zone access:off

	interface member:vlan 3 B#show security-access-rules security-access 100 from Trust to Untrust 10

26.2.4.3 Configuring a Global Access Policy for Security Zones

Configuration Effect

Global access policies globally control whether mutual access is allowed in a security zone and between security zones with the same priority. It also controls whether logs are generated in the case of connection release after a security zone policy is met or in the case of packet discarding because a security zone policy is not met.

Configuration Steps

- **Allowing Mutual Access Within a Security Zone**
  - (Optional) The configuration is required when intra–security zone access is allowed globally.
  - Perform the configuration in privileged EXEC mode.
- **Allowing Mutual Access Between Security Zones with the Same Priority**
  - (Optional) This configuration globally allows mutual access between security zones with the same priority when the inter–security zone access policy is not met.
  - Perform the configuration in privileged EXEC mode.
- **Configuring Log Generation in the Case of Connection Release After a Security Zone Policy Is Matched**
  - (Optional) This configuration globally enables log generation in the case of connection release after a security zone policy is met.
  - Perform the configuration in privileged EXEC mode.
- **Configuring Log Generation in the Case of Packet Discarding due to Violation of a Security Zone Access Policy**
  - (Optional) This configuration globally enables log generation in the case of packet discarding due to violation of a security zone policy.
  - Perform the configuration in privileged EXEC mode.

Verification

- Verify that the global **loose-inner-zone-access** command can be used to enable access control in the same security zone.
- Verify that the global **loose-inter-zone-access** command can be used to enable access control between two security zones with the same priority.
- Verify that the **security-permit-access-log** command can be used to configure log generation in the case of connection release after packet traffic matches a security zone policy.
- Verify that the **security-deny-access-log** command can be used to configure log generation in the case of packet discarding due to violation of a security zone access policy.

Related Commands

Globally Allowing IP Mutual Access Within a Security Zone When the Intra–Security Zone Access Policy Is Not Matched

Command	**loose-inner-zone-access**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	The priority of this command is lower than that of the **inner-zone-access** command.

Globally Allowing Mutual Access Between Security Zones with the Same Priority When the Inter-Security Zone Access Policy Is Not Matched

Command	**loose-inter-zone-access**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuring Log Generation in the Case of Connection Release After Packet Traffic Matches a Security Zone Policy

Command	**security-permit-access-log**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	This command is generally used for diagnosis.

Configuring Log Generation in the Case of Packet Discarding due to Violation of a Security Zone Access Policy

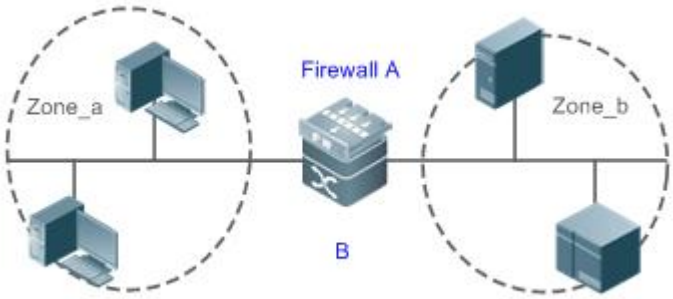
Command	**security-deny-access-log**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	This command is generally used for diagnosis.

Checking the Global Security Zone Access Policy

Command	**show security-access-global**
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	Global information shown by this command includes whether mutual access is globally allowed in a security zone and between security zones with the same priority. The following information is also displayed: security zone division method, whether logs are generated in the case of connection release after a security zone policy is matched, whether logs are generated in the case of packet discarding due to violation of a security zone access policy, and sequence number step for security zone access policy commands.

Configuration Example

Configuring Security Zone Division Based on IP Address Sets, Creating Two Security Zones, and Allowing Mutual Access Within and Between the Two Security Zones

Scenario Figure 266- 11	
Configuration Steps	● Configure the firewall to protect data flowing in and out of VLAN 3 (connected to zone_b) and configure VLAN 103 as a traffic diversion VLAN. ● Configure security zone division based on IP address set. Create two security zones: zone_a (for the network segment 192.168.1.0/24) and zone_b (for the network segment 192.168.2.0/24) and configure the same priority for the two security zones. Run the **loose-inner-zone-access** command to allow mutual access within the two security zones and run the **loose-inter-zone-access** command to allow mutual access between the two security zones. Enable the function of generating logs in the case of connection release after packet traffic matches a security zone policy and in the case of packet discarding due to violation of a security zone access policy.
B	B(config)#security-zone zone_a B(config-security-zone)#description Azone B(config-security-zone)#security-level 80 B(config-security-zone)#exit B(config)#security-zone zone_b B(config-security-zone)#description Bzone B(config-security-zone)#security-level 80 B(config-security-zone)#exit B(config)#loose-inner-zone-access B(config)#loose-inter-zone-access B(config)#security-permit-access-log B(config)#security-deny-access-log
Verification	Verify that mutual access is allowed within and between security zones zone_a and zone_b, and that logs are generated regardless of whether packets match a security zone policy.
B	B#show security-zone zone_a security-zone:zone_a description:Azone leve:80 inner-zone access:off B#show security-zone zone_b

	security-zone:zone_b description: Bzone level:80 inner-zone access:off B#show security-access-global security zone is base ip inner-zone access:on inter-zone access between same level:on permit access log:on deny access log:on access statistics:off access rule step:10

26.2.5 Monitoring

Displaying

Description	Command
Displays the configuration of a single or all security zones.	**show security-zone** [*zone-name*]
Displays global security zone access policies.	**show security-access-global**
Displays the IPv4 packet access policy of a security zone.	**show security-access-rules** { [**from** *zone-name1*] *firewall-name* | [**to** *zone-name2*] }
Displays the matching of a security zone policy based on IPv4 packet characteristics in security zones divided by interface.	**show security-zone-match** *ip-protocol source-ip dst-ip* **from** *src-interface* **to** *dst-interface*
Displays the matching of a security zone policy based on IPv4 TCP or UDP packet characteristics in security zones divided by interface.	**show security-zone-match** { **6** | **17** | **tcp** | **udp** } *source-ip dst-ip* [*src-port dst-port*] **from** *src-interface* **to** *dst-interface firewall-name*
Displays the matching of a security zone policy based on IPv4 ICMP packet characteristics in security zones divided by interface.	**show security-zone-match** { **1** | **icmp** } *source-ip dst-ip* [*type code*] **from** *src-interface* **to** *dst-interface firewall-name*

Chapter 12 WLAN QoS Configuration

1. Configuring WQoS
2. Configuring WMM

1 Configuring WQoS

1.1 Overview

WLAN QoS (WQoS) is a wireless bandwidth control technology. It involves rate limiting, fair scheduling, and anti-proxy check.

Rate limiting is used to limit the traffic of access points (APs), WLAN, or STAs, thus preventing the traffic from exceeding a specified range. Rate limiting is applicable to scenarios where some STAs occupy too much bandwidth and other STAs do not have sufficient bandwidth.

Fair scheduling, by dividing the time equally, resolves the problem that some nodes occupy the air interfaces for a longer time, particularly low-rate nodes. Fair scheduling is applicable to all wireless networks.

Anti-proxy check resolves the problem that some unauthorized STAs access a wireless network because a STA serves as their proxy. This function is applicable to scenarios where illegal proxy servers must be eliminated in a LAN.

Protocols and Standards

- IEEE 802.11e-2005: Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements, IEEE Computer Society
- Wi-Fi: WMM Specification version 1.1

1.2 Applications

Application	Description
Bandwidth Control in a Fit AP Architecture	A fit AP architecture is deployed with at least one access controller (AC) and one AP.

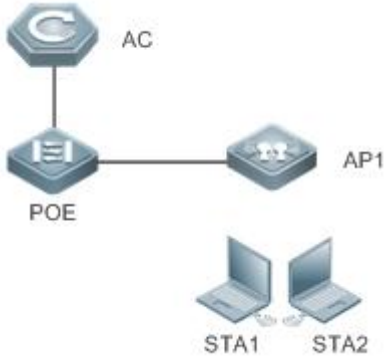
1.2.1 Bandwidth Control in a Fit AP Architecture

Scenario

On the wireless network, an AC is deployed to implement rate limiting on APs, WLANs, and STAs, and fair scheduling and anti-proxy check on APs.

As shown in Figure 1- 1, the AC implements rate limiting on APs, WLANs, and STAs, and fair scheduling and anti-proxy check on APs.

Figure 1- 1



Remarks	AC: Wireless access controller POE: Gateway switch for AP 1

	AP 1:Wireless access device STA 1 and STA 2: User devices

Deployment

- Enable WQoS on the AC.

1.3 Features

Basic Concepts

Rate Limiting

To better utilize the limited network resources and serve more users efficiently, the access device need to support rate limiting. When the traffic rate conforms to the committed rates, packets are allowed to pass; otherwise, packets are discarded.

The following parameters are used to evaluate the traffic:

- Average Data Rate: It is the average flow rate that is allowed. It is also called committed information rate (CIR).
- Burst Data Rate: It is the maximum acceptable rate of each burst data, also called committed burst size (CBS).The configured CBS must be greater than the maximum packet length, that is, the maximum rate at which data is sent in a period of 10 milliseconds. (The CBS in the unit of Kbps is equal to the maximum traffic in a period divided by 10 milliseconds).

Fair Scheduling

Fair scheduling allows STAs in the same frequency band of the same AP to share the wireless network resources provided by the AP fairly. The fair scheduling function can prevent low-speed STAs from decreasing the throughput of the entire wireless network, and provide smoother network experience for STAs. Besides, the fair scheduling function provides users with better experience by monitoring changes in the traffic of each STA intelligently and adjusting the proportion of the wireless bandwidth used by each STA dynamically. In software version later than 10.4(1T19)p1, different priorities can be configured for STAs in fair scheduling so that specified users can preferentially enjoy the wireless bandwidth.

Anti-Proxy Check

In software versions later than 10.4(1T19)p1, anti-proxy check is offered to detect whether some STAs in LAN serve as proxies of other STAs, thus accurately monitoring the number of STAs and network traffic.

Overview

Feature	Description
Rate Limiting	Limit the rates of an AP, a WLAN, or a STA to that the rate does not exceed the limit.
Fair Scheduling	Associate a STA with other STAs in the same frequency band of the same AP to share the wireless network resources provided by the AP, thus sharing the bandwidth of the wireless network in a fair manner.
Anti-proxy Check	Detect the STAs on an LAN that serve as proxies of other STAs, thus accurately monitoring the number of STAs and network traffic.

1.3.1 Rate Limiting

Rate limiting is used to limit the rates of an AP, a WLAN, or a STA to ensure that the rate does not exceed a certain range.

Working Principle

Rate limiting is implemented based on the token bucket.

- The token bucket records the number of bytes that can pass in a certain period of time.
- In each period, the number of data bytes that can pass is calculated based on the configured CIR and CBS, thereby adjusting the size of the token bucket.
- When a packet arrives, the packet size in bytes is compared with the size of the token bucket. When the packet size is smaller than that of the token bucket, the packet is allowed to pass, and the token bucket size decreases with the corresponding amount. When the packet size is greater than that of the token bucket, two processing methods are followed: (1) Packet buffering is also known as Traffic Shaping. The packet is buffered and transmitted after obtaining permission by the token bucket; (2) Traffic Policing: The packet is directly dropped. Traffic Shaping smoothens the traffic with low fluctuation; Traffic Policing results in big fluctuation of traffic.
- Currently, on an AP, Traffic Shaping is used to implement rate limiting of an AP, a STA, or a WLAN. On an AC, Traffic Policing is used to implement rate limiting of a WLAN.

1.3.2 Fair Scheduling

Fair scheduling, by dividing the time equally, resolves the problem that some nodes occupy the air interfaces for a longer time, particularly low-rate nodes.

Working Principle

Owing to the special characteristics of the wireless network, STAs (including APs) on the same network share the air interface resources, which is also a bottleneck of STA performance. This is one of the differences between the wired and wireless networks. Traditional packet scheduling often adopts the first in first out (FIFO) mode. On one wireless network, every STA that needs to transmit data want to occupy the air interface resources whenever possible. Transmission of overwhelming low-rate packets results in long-time occupation of the air interfaces. Thereby, the lasting queue take-up causes packet loss and degrades the overall performance of the network.

In the real wireless scenarios, STAs often differ in types and performance. Consequently, some STAs always cannot obtain the resources, or get super slow response. What is worse, these STAs cannot access the network, which seriously affects user experience.

To settle the problems, it is essential to ensure that each STA is able to obtain resources on air interfaces fairly. That is, every STA that needs to transmit data can occupy the air interfaces for a fair period of time. Fair scheduling of the wireless links can be achieved by ways as follows: Predict the traffic of every STA based on the STA-specific information (such as negotiated rates and aggregation types) and the valid bytes of packets, convert the traffic to the number of packets that can be transmitted by every STA, and adjust the allowed packet number to allocate the bandwidth to every STA over the air interfaces and implement traffic shaping. With fair scheduling, each STA occupies the air interfaces for an equal period of time, which effectively avoids poor performance of some STAs and thus improves user experience.

1.3.3 Anti-Proxy Check

Anti-proxy check resolves the problem that some unauthorized STAs can access the wireless network because legal STAs serve as their proxies.

Working Principle

Check whether the packets sent by STAs conform to the requirements for the proxy server's packets to determine whether the STAs serve as the proxy servers, and take countermeasures accordingly. Currently, two policies are supported:

- Time to Live (TTL) detection policy: On the AP, check whether the TTL field in an IP packet sent from a STA is in the valid range. If not, it is concluded that the STA is a proxy server.
- TCP source port detection policy: On the AP, check whether the number of ports used in a TCP packet sent by a STA is in the valid range. If not, it is concluded that the STA is a proxy server.

1.4 Configuration

Configuration	Description and Command	
Configuring Rate Limiting	(Mandatory) It is used to enable rate limiting.	
	ap-based	Configures AP-based rate limiting on an AC.
	netuser	Configures STA-based rate limiting on an AC.
	wlan-based	Configures WLAN-based rate limiting on an AC.
	wlan-qos ap-based	Configures AP-based rate limiting on an AP.
	wlan-qos netuser	Configures STA-based rate limiting on an AP.
	wlan-qos wlan-based	Configures WLAN-based rate limiting on an AP.
Configuring Fair Scheduling	(Mandatory) It is used to enable fair scheduling.	
	fair-schedule	Enables fair scheduling.
	(Optional) It is used to adjust the STA priority during fair scheduling.	
	sta-fair	Configures the fair scheduling priority of a STA.
Configuring Anti-Proxy Check	(Mandatory) It is used to configure the anti-proxy check policy.	
	illegal-sta-check ip ttl	Enables TTL detection policy for anti-proxy check.
	illegal-sta-check tcp source-ports	Enables TCP source port detection policy for anti-proxy check

1.4.1 Configuring Rate Limiting

Configuration Effect

- Only the committed resource is allocated to a stream based on the actual situation of the network, which prevents network congestion caused by burst stream.

Notes

- On a fat AP, CLI commands are configured in global configuration mode, and the prefix **wlan-qos** is added to the relevant commands.
- The rate limiting effect of the **wlan-based per-ap-limit** command configured on an AC is equivalent to that of the **wlan-qos wlan-based total-user-limit** command configured on all connected APs.
- The following types of rate limiting are available on STAs: **wlan-based per-user-limit**, **wlan-based per-ap-limit intelligent**, **ap-based per-user-limit**, **ap-based total-limit intelligent**, and **netuser**. However, only one type of them works at a time. From high to low, the priorities of these types of rate limiting are as follows: **netuser**>**wlan-based per-ap-limit intelligent** > **wlan-based per-user-limit** > **ap-based total-limit intelligent** > **ap-based per-user-limit**.

- Rate limiting, including **wlan-based total-limit**, **wlan-based per-ap-limit**, **ap-based total-limit**, and STA-based rate limiting, can take effect on different objects simultaneously without considering priorities.

Configuration Steps

Configuring AP-based Rate Limiting

- Mandatory.
- On a fat AP, run the **wlan-qos ap-based** command in global configuration mode to configure AP-based rate limiting.
- On an AC, run the **ap-based** command in AP configuration mode to configure AP-based rate limiting.

Command	**ap-based** { **per-user-limit** | **total-user-limit** [**intelligent**] } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*
Parameter Description	**per-user-limit**: Indicates that rate limiting is implemented on every STA on the AP. **total-user-limit**: Indicates that rate limiting is implemented on all STAs on the AP. **intelligent**: Indicates whether rate limiting is implemented on all STAs on the AP intelligently. **down-streams**: Indicates that rate limiting is implemented on the downlink traffic of the AP. **up-streams**: Indicates that rate limiting is implemented on the uplink traffic of the AP. *average-data-rate*: Indicates CIR. The unit is 8 Kbps. The value ranges from 8 to 261,120. *burst-data-rate*: Indicates CBS. The unit is 8 Kbps. The value ranges from 8 to 261,120.
Defaults	By default, rate limiting is not configured. If **total-user-limit** is configured, intelligent rate limiting is disabled by default.
Command Mode	AC: AP configuration mode Fat AP: Global configuration mode
Usage Guide	N/A

Configuring STA-based Rate Limiting

- Mandatory.
- On a fat AP, run the **wlan-qos netuser** command in global configuration mode to configure STA-based rate limiting.
- On an AC, run the **netuser** command in AC configuration mode to configure STA-based rate limiting.

Command	**netuser** *mac-address* { **inbound** | **outbound** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*
Parameter Description	*mac-address*: Indicates the MAC address of a STA. **inbound:** Indicates that rate limiting is implemented on the uplink traffic of a STA. **outbound:** Indicates that rate limiting is implemented on the downlink traffic of a STA. *average-data-rate*: Indicates CIR. The unit is 8 Kbps. The value ranges from 8 to 261,120. *burst-data-rate*: Indicates CBS. The unit is 8 Kbps. The value ranges from 8 to 261,120.
Defaults	By default, rate limiting is not configured.
Command Mode	AC: AC configuration mode Fat AP: Global configuration mode
Usage Guide	N/A

Configuring WLAN-based Rate Limiting

- Mandatory.
- On a fat AP, run the **wlan-qos wlan-based** command in global configuration mode to configure WLAN-based rate limiting.
- On an AC, run the **wlan-based** command in WLAN configuration mode to configure WLAN-based rate limiting.

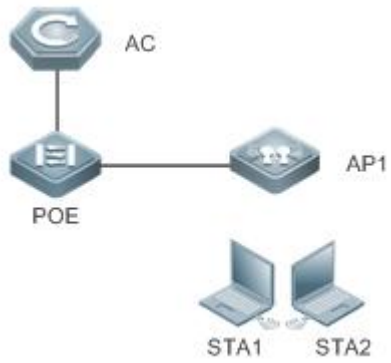
Command	**wlan-based** { **per-user-limit** | **total-user-limit** [**intelligent**] | **per-ap-limit** } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*
Parameter Description	**per-user-limit**: Indicates that rate limiting is implemented on every STA on the WLAN. **total-user-limit**: Indicates that rate limiting is implemented on all STAs on the WLAN. **intelligent**: Indicates whether rate limiting is implemented on all STAs on the WLAN intelligently. **per-ap-limit**: Indicates that AP-based rate limiting is implemented. **down-streams**: Indicates that rate limiting is implemented on the downlink traffic of the WLAN. **up-streams**: Indicates that rate limiting is implemented on the uplink traffic of the WLAN. *average-data-rate*: Indicates CIR. The unit is 8 Kbps. The value ranges from 8 to 261,120. *burst-data-rate*: Indicates CBS. The unit is 8 Kbps. The value ranges from 8 to 261,120.
Defaults	By default, rate limiting is not configured.
Command Mode	AC: WLAN configuration mode Fat AP: Global configuration mode
Usage Guide	N/A

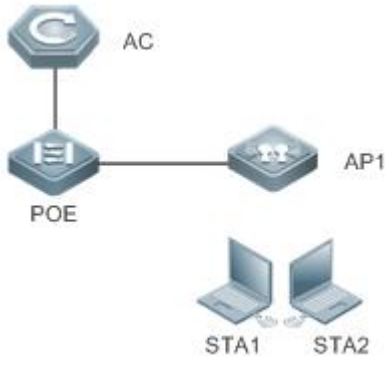
Verification

- Run the **show dot11 ratelimit ap** command to display the AP-based rate limiting information.
- Run the **show dot11 ratelimit user** command to display the STA-based rate limiting information.
- Run the **show dot11 ratelimit wlan** command to display the WLAN-based rate limiting information.

Configuration Example

Configuring AP-based Rate Limiting

Scenario Figure 1- 2	
Configuration Steps	● In AP configuration mode, configure AP-based, STA-based, and downlink rate limiting.
AC	FS#configure terminal FS(config)# ap-config ap1 FS(config-ap)#ap-based per-user-limit down-streams average-data-rate 100000 burst-data-rate 120000 FS(config-ap)# exit
Verification	Run the **show dot11 ratelimit ap** command to display the configurations.

Scenario Figure 1- 2	
Configuration Steps	● In AP configuration mode, configure AP-based, STA-based, and downlink rate limiting.
AC	FS#configure terminal FS(config)# ap-config ap1 FS(config-ap)#ap-based per-user-limit down-streams average-data-rate 100000 burst-data-rate 120000 FS(config-ap)# exit
Verification	Run the **show dot11 ratelimit ap** command to display the configurations.
AC	AC_20_3F#show dot11 ratelimitap AP name :test, ratelimit info(unit :8kbps): Per-user-limit: Upstream : average rate - 0 , burst rate - 0 Downstream : average rate - 100000, burst rate - 120000 Total-user-limit: Upstream : average rate - 0 , burst rate - 0 Downstream : average rate - 0 , burst rate - 0

1.4.2 Configuring Fair Scheduling

Configuration Effect

- The fair scheduling function can prevent low-speed STAs from decreasing the throughput of the entire wireless network, and provide smoother network experience for STAs.

Notes

- On a fat AP, configure fair scheduling in global configuration mode, and run the **show running-config** command to display the configurations.
- In fit AP mode, configure fair scheduling only on an AC.

Configuration Steps

Enabling Fair Scheduling

- Mandatory.
- On an AC, run the **fair-schedule** command in AP configuration mode to enable fair scheduling.
- On a fat AP, run the **fair-schedule** command in global configuration mode to enable fair scheduling.
- Enabling fair scheduling can allocate time to STAs in a fair manner.

Command	**fair-schedule**
Parameter Description	N/A
Defaults	By default, fair scheduling is enabled.
Command Mode	Fit AP: AP configuration mode Fat AP: Global configuration mode
Usage Guide	N/A

Configuring the Fair Scheduling Priority

- (Optional) Perform this configuration if you need to change the fair scheduling priority of a STA.
- On an AC, run the **sta-fair** command in AC configuration mode to configure the fair scheduling priority.
- On a fat AP, run the **sta-fair** command in global configuration mode to configure the fair scheduling priority.

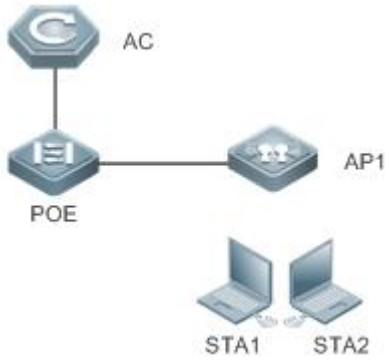
Command	**sta-fair** *mac-address* **priority** *priority*
Parameter Description	*mac-address*: Indicates the MAC address of a STA. *priority*: Indicates the priority. The value ranges from 1 to 6.
Defaults	By default, the priority is 1 for all STAs. A greater value indicates a higher priority, and a higher priority indicates that a longer time is allocated to the STA.
Command Mode	Fit AP: AC configuration mode Fat AP: Global configuration mode
Usage Guide	N/A

Verification

- Run the **show ap-config run** command to display the configurations.

Configuration Example

Enabling Fair Scheduling and Configuring the Priority

Scenario Figure 1- 3	
Configuration Steps	● In AP configuration mode, enable fair scheduling. ● In AC configuration mode, configure the fair scheduling priority of a STA.
AC	FS#configure terminal FS(config)# ap-config ap1 FS(config-ap)#fair-schedule FS(config-ap)# exit FS(config)#ac-controller FS(config-ac)#sta-fair 1111.1111.1111 priority 6 FS(config-ac)# end
Verification	Run the **show ap-config running** and **show running-config** commands to display the configurations.
AC	FS# show ap-config running ! ap-configap1 ! FS# show running-config ! ac-controller sta-fair 1111.1111.1111 priority 6 !

1.4.3 Configuring Anti-Proxy Check

Configuration Effect

- Detect the STAs on a LAN that serve as proxies of other STAs, thus accurately monitoring the number of STAs and network traffic.

Configuration Steps

Enabling Anti-Proxy Check

- (Mandatory) The TTL detection policy or the TCP source port detection policy can be adopted.

- On an AC, run the **illegal-sta-check** command in AP configuration mode to enable anti-proxy check.
- With this function enabled, the AC can check whether a STA serves as the proxy server of another STA, and take countermeasures accordingly.
- Enable TTL detection policy for anti-proxy check.

Command	**illegal-sta-check ip ttl**
Parameter Description	N/A
Defaults	By default, anti-proxy check is disabled.
Command Mode	AP configuration mode
Usage Guide	N/A

- Enable TCP source port detection policy for anti-proxy check.

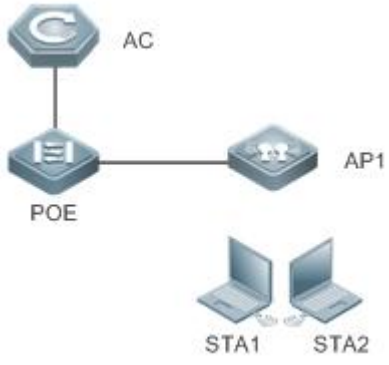
Command	**illegal-sta-check tcp source-ports** [*port-num*]
Parameter Description	*port-num*: Indicates the maximum number of ports that can be detected. The value ranges from 1 to 512.
Defaults	By default, anti-proxy check is disabled.
Command Mode	AP configuration mode
Usage Guide	N/A

Verification

- Run the **show running-config** command to check the configurations.

Configuration Example

Enabling Anti-Proxy Check

Scenario **Figure 1-4**	
Configuration Steps	• In AP configuration mode, enable anti-proxy check.
AC	FS#configure terminal FS(config)# ap-configap1 FS(config-ap)# illegal-sta-check ipttl

	FS(config-ap)# illegal-sta-check tcp source-ports FS(config-ap)# end
Verification	Run the **show ap-config running** command to display the configurations.

AC	FS# show ap-config running ap1
	!
	ap-configap1
	  illegal-sta-check ipttl
	  illegal-sta-check tcp source-ports
	!

1.5 Monitoring

Displaying

Description	Command
Displays the WQoS rate limiting information.	**show dot11 ratelimit** {**wlan** | **ap** | **user** }

2 Configuring WMM

2.1 Overview

WMM is a wireless QoS protocol, and this protocol is a subset of the 802.11e protocol.

WMM is used to ensure that high-priority packets are preferentially sent, thereby assuring the quality of the voice and video applications in a wireless network.

This document consists of two parts, that is, WMM service and QoS packet priority mapping.

- WMM service: The WMM service is used to differentiate the capabilities of the access channels with different priorities, thereby ensuring that channel resources are allocated based on data flow priorities. Users can adjust the values of the EDCA parameters for the client or AP based on actual requirements to make the AC with a higher priority to start the backoff process earlier than other ACs and preferentially access the channel.
- QoS packet priority mapping: Wireless-to-Wired QoS mapping and wired-to-wireless QoS mapping help to implement end-to-end QoS in the entire network, thereby assuring the quality of high-priority service flows.

Protocols and Standards

- IEEE 802.11e-2005: Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements, IEEE Computer Society
- RFC5416: Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE802.11

2.2 Applications

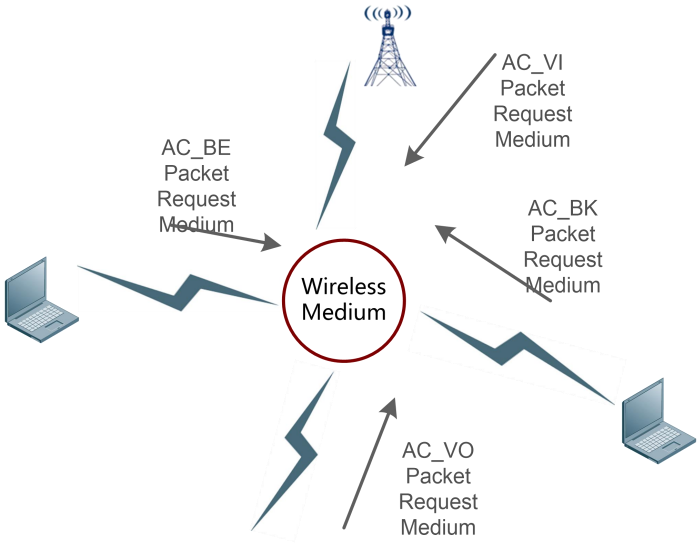
Application	Scenario
WMM Service Scenario	Competition process of channels with different priorities.
Wireless-to-Wired Priority Mapping Scenario	Wireless-to-wired QoS packet priority mapping process.
Wired-to-Wireless Priority Mapping Scenario	Wired-to-wireless QoS packet priority mapping process.

2.2.1 WMM Service

Scenario

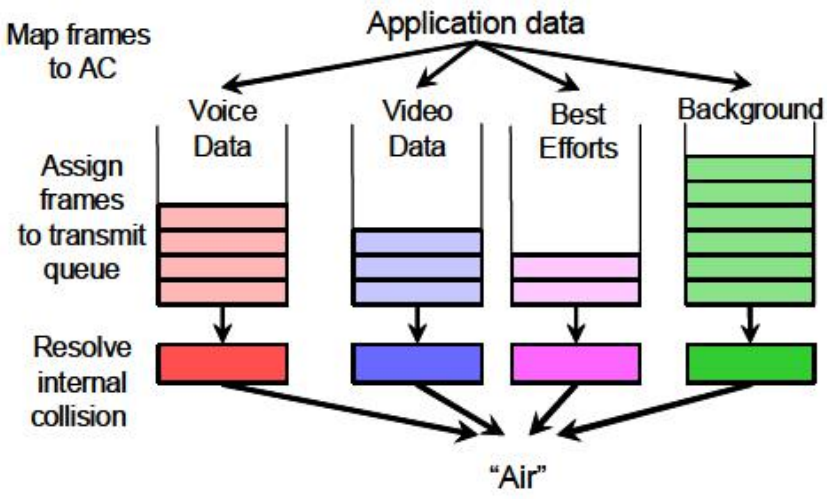
The medium for wireless communication is radio. In a specified frequency band, channels are shared during wireless network communication. In the same RF environment, the uplink and downlink traffic of different sites conflicts. Therefore, the problem how communication participants compete for shared channels needs to be solved to ensure wireless QoS. As shown in Figure 2-1, there are packets of four different priorities in the same wireless network environment (the packets from high priority to low are as follows: AC_VO > AC_VI > AC_BE > AC_BK). When multiple supplicants request the medium to send packets and compete for channels, the competition and coordination mechanism is enabled to determine which supplicant's packet can access the medium. The higher the packet’s priority is, the more likely the packet is to access the channel.

Figure 2-1 Channel competition



In a wireless network, since the medium is special, packet damage caused by packet loss and signal interference occurring during transmission over the network is quite serious. Different wireless transmission parameters of the mechanism need to be retransmitted to ensure arrival of packets. However, it is unpractical that preferable parameters are adopted for all packets. In this case, to provide services having high reliability and timeliness requirements, you can classify packets. In short, provide network services of different quality based on various requirements. That is, process key data packets having high timeliness requirement preferentially, and assign a low processing priority to general packets not having high timeliness requirement. To make a network carry different services, you must ensure that the network not only provides single service with the best QoS, but also provides different service with different QoS. Therefore, the QoS of a wireless AP requires the classification/identification of packets for identifying different data flows and providing service of different quality.

Figure 2-2 Wireless QoS multi-priority queue



Deployment

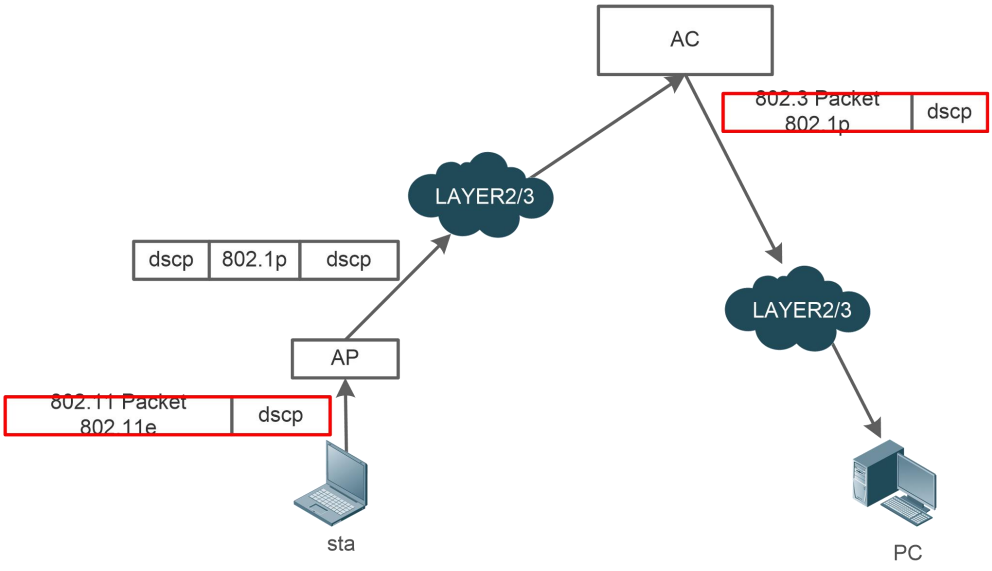
The device should be configured with the following key points:

- Enable the WMM.
- Set WMM EDCA competition parameters. Generally, default values are adopted.

2.2.2 Wireless-to-Wired Priority Mapping

Scenario

Figure 2-3 Wireless-to-wired packet priority mapping



STA-to-PC priority mapping process:

- STA sends an 802.11 packet carrying 802.11e and DSCP information to the AP.
- The AP sets the internal priority of the packet based on the trust mode of the wireless port (configured on the ESS of the AC based on the BSSID). If the trusted packet is with an 802.11e priority, the AP converts the packet with the 802.11e priority into a wired packet with the 802.1p and DSCP priorities and a CAPWAP encapsulated packet with the 802.1p and DSCP priorities. If the trust mode is DSCP priority, the preceding setting shall be performed based on the DSCP priority of the incoming wireless packet. Currently, the default ETH trust mode is DSCP, and the wireless end always maps to the dot11e.
- When passing layer 2/3 network, the CAPWAP packet is processed according to the wired QoS method.
- After receiving the CAPWAP packet, the AC decapsulates the packet and then forwards the wired packet generated after the decapsulation to the layer 2/3 network.
- When passing layer 2/3 network, the wired packet is processed according to the wired QoS method.

Deployment

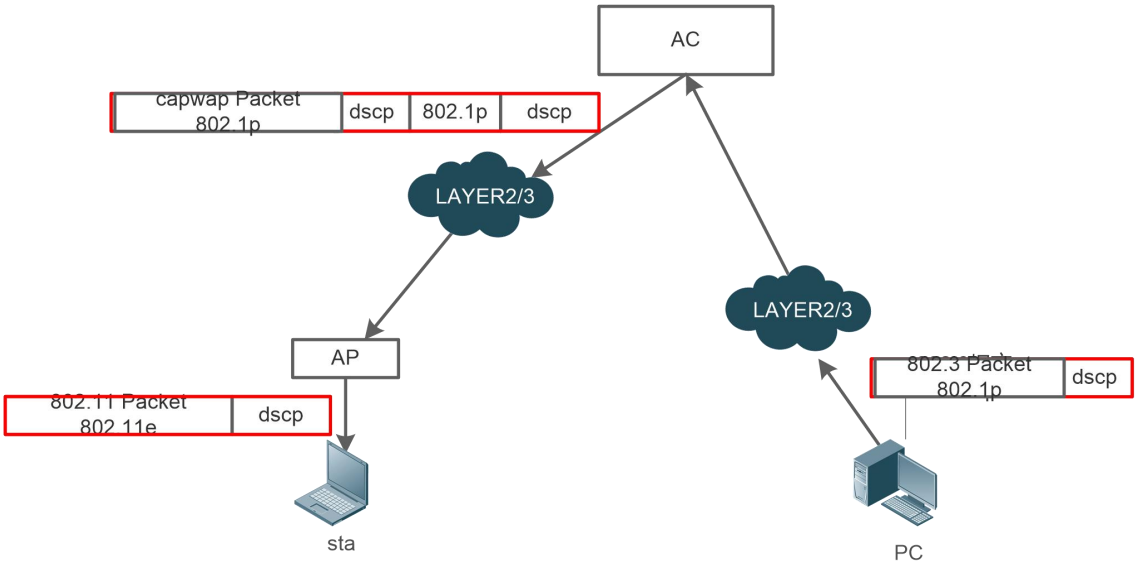
The device should be configured with the following key points:

- Enable the WMM.
- Set the wireless-to-wired priority mapping table. Generally, default values are adopted.

2.2.3 Wired-to-Wireless Priority Mapping

Scenario

Figure 2-4 Wired-to-wireless packet priority mapping



PC-to-station QoS mapping process:

- The AC receives an 802.3Mac packet from the PC.
- Set the internal COS priority of the packet based on the trust mode of the physical port. If the trusted packet has the 802.1p priority and carries tag, set the internal COS priority of the packet based on the 802.1p priority. Otherwise, set the default priority of the packet based on the default priority of the port. If the trust mode is DSCP priority, the preceding setting shall be performed based on the DSCP priority of the incoming wireless packet. Currently, the default ETH trust mode is DSCP, and the wireless end always maps to the dot11e.
- The AC encapsulates the 802.3 packet into a CAPWAP packet.
- After receiving the CAPWAP packet, the AP decapsulates the packet and performs QoS priority mapping for the wired-to-wireless packet generated after decapsulation based on the trust mode of QoS priority. If the trust mode is DSCP, the AP configures 802.11e and DSCP filed of the wireless packet based on the DSCP field value of the 802.3 packet. If the trust mode is 802.1p, the AP performs relevant settings based on the COS field of the 802.3 packet.
- Based on the 802.11e priority of the wireless packet, the AP participates in the competition for wireless channels and sends the wireless packet to the STA.

Deployment

The device should be configured with the following key points:

- Enable the WMM.
- Set the wired-to-wireless priority mapping table. Generally, default values are adopted.

2.3 Features

Basic Concepts

Access Class

According to the WMM standard, access data flows have four priorities. Each priority can be regarded as a class. From the lowest priority to the highest priority, the sequence is as follows: AC_BK, Background < AC_BE, Best Efforts < AC_VI, Video Data < AC_VO, Voice Data.

EDCA Competitive Mechanism

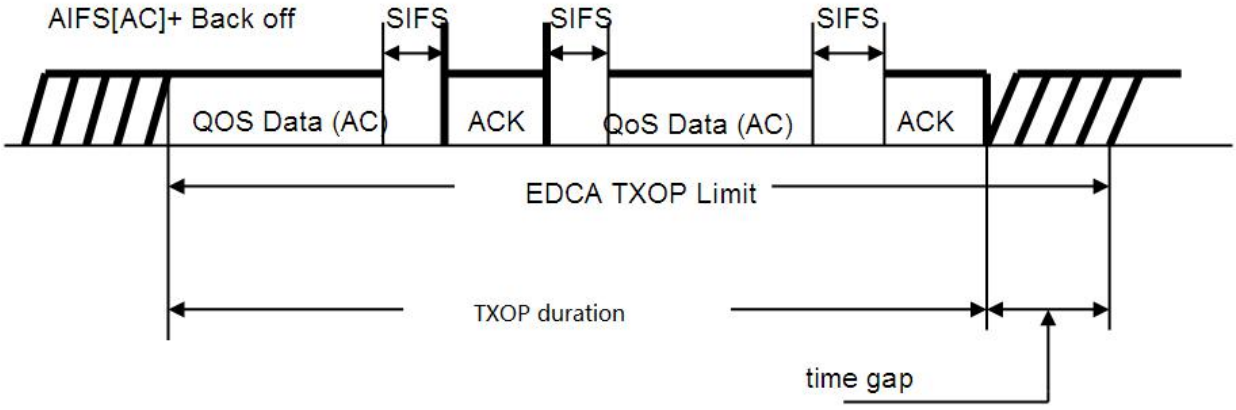
The EDCA competitive mechanism is the core of the IEEE 802.11e. The EDCA differentiates the access capabilities of AC channels with different priorities, ensuring that air interface resources are allocated based on data flow priorities. Enhanced distributed channel access (EDCA) not only retains distributed channel competition between the AP and STA, but also introduces internal competition of four internal priority classes of QAP/QSTA. In this way, EDCA introduces the channel competition mechanism for differentiating the priority classes between different QAPs and QSTAs through the wireless air interface. Competition for channels is implemented by configuring EDCA competition parameters of different priority classes. The QAP pushes the configuration to the QSTA and controls the access capability of the QSTA. Competition parameters include AIFS, TXOP Limit, CWmin, and CWmax.

EDCA Parameters

The EDCA competition parameters are listed as follows:

- AIFSN (Arbitration Inter Frame Spacing Number): In the 802.11 protocol, the Distributed Inter-frame Spacing (DIFS) is a fixed value. However, the DIFS for different ACs of the WMM can be set to different values. A larger AIFSN value means a longer DIFS. A shorter DIFS means a bigger probability of preempting channels.
- ECWmin (Exponent form of CWmin) and ECWmax (Exponent form of CWmax) determine the average backoff time. Larger ECWmin and ECWmax mean a longer backoff time.
- TXOP (Transmission Opportunity): maximum duration for preempting channels after successful competition by a user at one time. A larger TXOP means a longer duration for a user to preempt channels. If the TXOP value is 0, only one packet is sent after channel preemption each time. If a frame is too large to be completely sent within the TXOP, this frame must be segmented.

Figure 2-5 TXOP successive frame transmission



ACK Policy

Two ACK policies are available, that is, Normal ACK and No ACK.

- Normal ACK: After receiving a unicast packet successfully, the recipient returns an ACK response.
- No ACK: In the environment with high communication quality and little interference, you can configure the mechanism of not returning an ACK packet for the flow of a certain priority for confirmation, saving the channel resource. During wireless packet

interaction, it is not necessary that an ACK packet is used for confirmation. The No ACK policy helps to improve the transmission efficiency effectively. However, it may cause packet loss.

According to the IEEE 802.11 standard, no ACK is returned for multicast or broadcast frames.

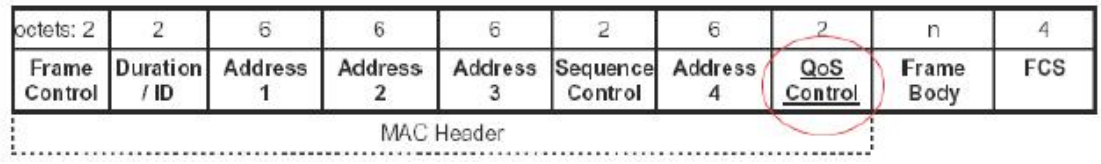
AC Queue Depth

If the queue depth of packets of a certain priority is greater than the preset AC queue depth, subsequent packets are discarded. Otherwise, subsequent packets are added to the queue for processing according to normal logics.

802.11e Priority

802.11e extends the MAC header of 802.11, with the QoS Control domain added, as shown in Figure 2-6.

Figure 2-6 802.11e MAC Header



The QoS Control domain has two bytes. Among them, the first three bits are the TID field, indicating the data form identification code. TID values 0-7 are used for QoS with priorities, indicating the priorities (UP) of users; TID values 8-15 are used for parameter-based QoS, indicating the data flow ID (TSID).

The WMM maps UP to corresponding AC. The following table lists the mapping between the 802.11e priority and AC.

Priority	UP (User Priority)	AC (Access Category)
Lowest	1	Back-ground
	2	Back-ground
	0	Best-effort
	3	Best-effort
	4	Video
	5	Video
	6	Voice
Highest	7	Voice

Priority Mapping Table

After a packet enters a device, the device judges the packet trust mode of the current interface, that is, judges which part of priority information in the received packet is valid. In addition, the device judges the work mode (fat AP or fit AP) of the current AP. Then, the device selects a mapping table based on the preset information to perform the priority mapping operation.

Overview

Feature	Description
WMM Service	Configure WMM service, including EDCA competition parameters, AC queue depth, and ACK policy.
QoS Packet Priority Mapping	Configure QoS packet priority mapping, including the QoS packet priority mapping table and priority mapping policy.

2.3.1 WMM Service

Configure WMM service, including EDCA competition parameters, AC queue depth, and ACK policy.

Working Principle

Provide network services of different quality based on various requirements. That is, provide high-quality services for key data packets having high timeliness requirement and process them preferentially, and assign a low processing priority to common packets not having high timeliness requirement. According to the WMM standard, access data flows have four priorities. Each priority can be regarded as a class. The EDCA differentiates the access capabilities of AC channels with different priorities, ensuring that air interface resources are allocated based on data flow priorities.

Enabling WMM

Enable/disable the WMM service. When the WMM service is enabled, the four-level priority queue is used for reception and mapping. When the WMM service is disabled, the default priority queue is used for reception and mapping.

EDCA Competitive Mechanism, AC Queue Depth, and NO ACK Policy

- EDCA competitive mechanism:

EDCA parameters differentiate the channel access capabilities of different priorities. Each AC has its own EDCA channel competition parameters. Users can adjust the values of the EDCA parameters on the client or AP based on actual requirements to make the AC with a higher priority to start the backoff process earlier than other ACs and preferentially access the channel. The channel competition should be completed automatically by the hardware. The hardware would be engaged in the channel competition after parameters such as CWmin, CWmax, AIFSN, TXOP of each hardware queue are set on the software.

During actual configuration, you can choose to configure the EDCA parameters on the client side or AP side based on application requirements. The configuration of edca-client mainly affects the wmm competition parameters of sta, and the configuration of edca-radio mainly affects the wmm competition parameters of AP.

The QSTA configuration is managed and pushed by the QAP in a centralized manner. The channel competition parameters of QAP and QSTA are mutually independent. Generally, the channel competition parameters of QAP would be slightly increased to ensure competent channel control capability for QAP. QAP would notify the EDCA parameter setting of QAP through the EDCA Parameter Set IE of the frame of beacon or Probe Response, and push the negotiated EDCA configuration to QSTA through EDCA Parameter Set IE of the (Re)Association Response frame.

- AC queue depth:

Set the AC queue depth. If the queue depth of packets of a certain priority is greater than the preset AC queue depth, subsequent packets are discarded. Otherwise, subsequent packets are added to the queue for processing according to normal logics.

- NO ACK policy:

Enable/disable the NO ACK (No Acknowledgement) policy. The NO ACK policy should be supported by the recipient and the sender at the same time. When the NO ACK policy frame transmission chip does not support NO ACK policy for a queue, the NO ACK policy should be set in the DMA descriptor of each frame sent at each frame sent.

The NO ACK policy is used as an alternative for the method of receiving confirmation (during wireless packet exchange) by using ACK packets in the environment with high communication quality and little interference. The NO ACK policy helps to effectively improve the transmission efficiency. However, if ACK packet for confirmation is not used and the communication quality is poor, the sender would not retransmit the packets even if the recipient has not received the packets, resulting in increasing packet loss rate.

2.3.2 QoS Packet Priority Mapping

Configure QoS packet priority mapping, including the QoS packet priority mapping table and priority mapping policy.

Working Principle

The priority mapping tables provided by the device correspond to relevant priority mapping respectively. Then, a mapping table is selected based on the preset information to perform the priority mapping operation, thereby implementing end-to-end QoS for the entire network.

Packet Priority Mapping

In the IP network, IPv4 packets carry QoS priority tags in three modes, that is, layer 2-based CoS field (IEEE802.1p) priority, IP layer-based IP priority field ToS priority, and IP layer-based DSCP (Differentiated Services Codepoint) field priority.

For the three QoS priority tags of wired packets, it is sufficient to support the two kinds of QoS (DSCP and dot1P) because DSCP is compatible with ToS. In addition to the preceding three modes, the QoS priority tag mode of dot11e is also available for wireless packets.

As for the determination and execution of packet priority mapping, the device judges the packet trust mode or tag policy of the current interface, that is, judges which part of priority information in the received packet is valid. In addition, the device judges the work mode (centralized forwarding or local forwarding) of the current AP. Then, the device selects a mapping table based on the preset information to perform the priority mapping operation.

2.4 Configuration

Configuration	Description and Command	
Configuring the WMM Service	(Mandatory). It is used to enable the WMM service.	
	wmm enable	Enables the WMM service.
	(Optional). It is used to configure competition parameters.	
	wmm edca-client	Configures the EDCA parameters for the client.
	wmm edca-radio	Configures the EDCA parameters for the AP.
Configuring the QoS Packet Priority Mapping	(Optional). It is used to configure the priority mapping. Mapping command for non-interworking versions.	
	wlan-qos map-table	Configures packet priority mapping of the current WLAN.
	(Optional). It is used to configure the 802.11p QoS mapping policy mechanism. Mapping command for interworking versions.	
	wmm dot1p enable	Enables 802.11p QoS mapping policy mechanism.
	wmm dot1p policy 1q	Configures how to apply the 802.11p QoS mapping policy mechanism for the AP.
	wmm dot1p tag	Configures 802.1p priority.

Configuration	Description and Command	
	(Optional) . It is used to configure the DSCP QoS mapping policy mechanism. Mapping command for interworking versions.	
	wmm dscp enable	Enables DSCP QoS mapping policy mechanism.
	wmm dscp policy outer-tunnel inner-tunnel	Configures how to apply the DSCP QoS mapping policy mechanism for the AP.
	wmm dscp tag	Configures DSCP identifications.

2.4.1 Configuring the WMM Service

Configuration Effect

- Configure the EDCA competition parameters for the client.
- Configure the EDCA competition parameters for the AP.
- Configure the ACK policy.
- Configure the length of the priority queue.

Notes

- The parameter configuration takes effect after the WMM service is enabled.
- When the WMM service is enabled and the BE queue adopts the default configuration, the Xspeed function dynamically adjusts the parameters of the BE queue.

Configuration Steps

Enabling the WMM Service

- Mandatory configuration.
- Run the **wmm enable radio** *radio-id* command in AP configuration mode and interface configuration mode to enable the WMM for the fit AP and fat AP respectively.
- When the WMM service is enabled, the four-level priority queue is used for reception and mapping. When the WMM service is disabled, the default priority queue is used for reception and mapping.

Command	**wmm enable radio** *radio-id*
Parameter Description	**radio** *radio-id*: Indicates that radio of the enabled/disabled WMM service is selected. Value range: 1-48. This parameter is not available on the fat AP. Only the AC supports configuration of this parameter.
Defaults	WMM is enabled by default
Command Mode	Configure this parameter in AP configuration mode on the fit AP and interface configuration mode on the fat AP.
Usage Guide	When the WMM service is disabled, the default priority queue is used for reception and mapping.

Configuring the EDCA Parameters for the Client

- Optional configuration.

By default, the EDCA parameters on the client side are as follows:

AC	aifs	cwmin	cwmax	txop
back-ground	7	4	10	0
best-effort	3	4	10	0
video	2	3	4	94
voice	2	2	3	47

After the EDCA parameters on the client side and AC queue depth are set, relevant processing is conducted based on the settings. Otherwise, processing is conducted based on the default settings.

Command	**wmm edca-client** { **back-ground** | **best-effort** | **video** | **voice** } { **aifsn** [*aifsn-value*] **cwmin** [*cwmin-value*] **cwmax** [*cwmax-value*] **txop** [*txop-value*] | **length** [*queue-length*] } **radio** *radio-id*
Parameter Description	**back-ground**: Sets the back-ground queue. **best-effort**: Sets the best-effort queue. **video**: Sets the video queue. **voice**: Sets the voice queue. **aifsn** *aifsn-value*: Sets the aifsn value. Value range: 1-15. **cwmin** *cwmin-value*: Sets the cwmin value. Value range: 0-15. **cwmax** *cwmax-value*: Sets the cwmax value. Value range: 0-15. **txop** *txop-value*: Sets the txop value. Value range: 0-255, unit: 32 μs. **length** *queue-length*: Sets the AC queue length. Value range: 1-255. The default is 255. **radio** *radio-id*: Sets radio of the EDCA parameters on the client. Value range: 1-48. This parameter is not available on the fat AP. Only the AC supports configuration of this parameter. **no**: Restores the default settings.
Command Mode	Configure these parameters in AP configuration mode on the fit AP and interface configuration mode on the fat AP.
Usage Guide	The parameter configuration takes effect only when the WMM service is enabled. The cwmax value must be greater than the cwmin value. Otherwise, a configuration error message is displayed.

Configuring the EDCA Parameters for the AP

- Optional configuration.
- By default, the EDCA parameters on the AP side are as follows:

AC	aifs	cwmin	cwmax	txop
back-ground	7	4	10	0
best-effort	3	4	6	0
video	1	3	4	94
voice	1	2	3	47

After the EDCA parameters on the AP side and NO ACK policy are set to non-default settings, relevant processing is conducted based on the settings. Otherwise, processing is conducted based on the default settings.

Smaller AIFS of a high-priority AC means earlier backoff process. Smaller CWmin and CWmax values mean shorter backoff time. TXOP limit allows an AC to transmit multi-frame packets on it continuously within the SIFS interval after preempting a transmission opportunity. A larger TXOP limit means a lower packet conflict rate and a lower waste of air interface resources.

Command	**wmm edca-radio** { **back-ground** | **best-effort** | **video** | **voice** } { **aifsn** [*aifsn-value*] **cwmin** [*cwmin-value*] **cwmax** [*cwmax-value*] **txop** [*txop-value*] | **noack** } **radio** *radio-id*
Parameter Description	**back-ground**: Sets the back-ground queue. **best-effort**: Sets the best-effort queue. **video**: Sets the video queue. **voice**: Sets the voice queue. **aifsn** *aifsn-value*: Sets the aifsn value. Value range: 1-15. **cwmin** *cwmin-value*: Sets the cwmin value. Value range: 0-15. **cwmax** *cwmax-value*: Sets the cwmax value. Value range: 0-15. **txop** *txop-value*: Sets the txop value. Value range: 0-255, unit: 32 μs. **noack**: Indicates that the no ack policy is enabled. The no ack policy is disabled by default. **radio** *radio-id*: Sets radio of the EDCA parameters on the client. Value range: 1-48. This parameter is not available on the fat AP. Only the AC supports configuration of this parameter. **no**: Restores the default settings.
Command Mode	Configure these parameters in AP configuration mode on the fit AP and interface configuration mode on the fat AP.
Usage Guide	The parameter configuration takes effect only when the WMM service is enabled. The cwmax value must be greater than the cwmin value. Otherwise, a configuration error message is displayed.

Verification

- You can run the **show run** command on the fat AP or the **show run**/**show ap-config run** command on the fit AP to display the WMM service status. The EDCA parameters of the client that already take effect and the EDCA parameters used for the AP are not displayed when they adopt default settings.
- Capture packets to display the EDCA parameters of the client.

Configuration Example

Configuring WMM Service Parameters

Configuration Steps	• Enable/disable the WMM service on the AP. • Configure the EDCA parameters for the client. • Configure the EDCA parameters for the AP.
	FS # configure terminal FS(config)# ap-config AP001 FS(config-ap)# wmm enable radio 1 FS(config-ap)# wmm edca-client voice aifsn 2 cwmin 2 cwmax 3 txop 50 radio 1 FS(config-ap)# wmm edca-radio voice aifsn 1 cwmin 1 cwmax 3 txop 50 radio 1
Verification	Run the **show run** command on the fat AP or the **show run**/**show ap-config run** command on the fit AP to display the EDCA parameters of the client that already take effect and the EDCA parameters used for the AP. These parameters are not displayed when they adopt default settings.

Common Errors

- If no radio exists, an error message is displayed.
- The performance is affected if EDCA parameters are improperly configured. For example, if the value of a low-priority parameter is higher than that of a high-priority parameter, the performance of the high priority is affected.

2.4.2 Configuring the QoS Packet Priority Mapping

Configuration Effect

- Configure packet priority mapping for the current WLAN.
- Configure 802.11p QoS mapping policy mechanism.
- Configure DSCP QoS mapping policy mechanism.

Notes

- QoS packet priority mapping takes effect after the WMM service is enabled.

Configuration Steps

By default, the mapping from DSCP to 802.11e is as follows:

DSCP	802.11e
0-7	0
16-23	1
24-31	2
8-15	3
32-39	4
40-47	5
48-55	6
56-63	7

By default, the mapping from 802.11e to DSCP is as follows:

802.11e	DSCP
0	0
3	8
1	16
2	24
4	32
5	40
6	48
7	56

Configuring Packet Priority Mapping for the Current WLAN

- Optional configuration.
- Unless otherwise specified, packet priority mapping of the current WLAN shall be configured on all APs.

After the priority mapping and the value corresponding to the mapping table are set, relevant processing is conducted based on the settings. Otherwise, processing is conducted based on the default settings.

Command	**wlan-qos map-table** { **dot11e-inner-dscp** | **dot11e-tunnel-dscp** | **dscp-dot11e** } **import** *import-tag-value* **export** *export-tag-value*

Parameter Description	**dot11e-inner-dscp**: Sets priority mapping from dot11e to internal DSCP. **dot11e-tunnel-dscp**: Sets priority mapping from dot11e to CAPWAP DSCP. **dscp-dot11e**: Sets priority mapping from dscp to dot11e. **import** *import-tag-value*: Sets priority of the incoming original packet. **export** *export-tag-value*: Sets priority of the outgoing packet. **no**: Restores the default setting.
Command Mode	WLAN configuration mode
Usage Guide	This command is a mapping command for non-interworking versions. The parameter configuration takes effect only when the WMM service is enabled. The fat AP does not support dot11e-tunnel-dscp, and dot11e-inner-dscp is dot11e-dscp.

Enabling 802.11p QoS Mapping Policy Mechanism

- Optional configuration.
- Unless otherwise specified, DSCP QoS mapping policy mechanism shall be disabled on all APs.

When the 802.11p QoS policy mechanism is enabled, the mapping table related to 802.11p QoS is used. When the 802.11p QoS policy mechanism is disabled, the default mapping policy is adopted.

Command	**wmm dot1p enable radio** *radio-id*
Parameter Description	**radio** *radio-id*: Indicates that radio of the enabled/disabled 802.11p QoS mapping policy mechanism is selected. Value range: 1-48. This parameter is not available on the fat AP. Only the AC supports configuration of this parameter. **no**: Restores the default settings.
Command Mode	Configure these parameters in AP configuration mode on the fit AP and interface configuration mode on the fat AP.
Usage Guide	The parameter configuration takes effect only when the WMM service is enabled.

Configuring How to Apply the 802.11p QoS Mapping Policy Mechanism for the AP

- Optional configuration.
- Unless otherwise specified, the 802.11p QoS mapping policy mechanism application shall be performed on all APs.

Determine where shall the 802.1Q priority be obtained based on the configuration determining how the AP applies the 802.11p QoS mapping policy mechanism.

Command	**wmm dot1p policy 1q** [*1q-policy-value*] **radio** *radio-id*
Parameter Description	**1q** *1q-policy-value*: Indicates setting for applying the 802.11p QoS mapping policy mechanism. Value range: 0-1. The default is **0**. **radio** *radio-id*: Indicates how the AP applies radio of 802.11p QoS mapping policy mechanism. Value range: 1-48. This parameter is not available on the fat AP. Only the AC supports configuration of this parameter. **no**: Restores the default settings.
Command Mode	Configure these parameters in AP configuration mode on the fit AP and interface configuration mode on the fat AP.
Usage Guide	The parameter configuration takes effect only when the WMM service is enabled. The configuration for applying the 802.11p QoS mapping policy mechanism takes effect only when the 802.11p QoS mechanism is enabled.

Configuring 802.1p Priority

- Optional configuration.

- Unless otherwise specified, 802.1p priority shall be configured on all APs.

Determine the priority of 802.1p based on the configuration of 802.1p priority.

Command	**wmm dot1p tag** [*tag-value*] { **back-ground** | **best-effort** | **video** | **voice** } **radio** *radio-id*
Parameter Description	**tag** *tag-value*: Sets the 802.1p priority. Value range: 0-7. The default **best-effort** is **0**; the default ;**back-ground** is **2**; the default **video** is **4**; the default **voice** is **6**. **back-ground**: Sets the back-ground queue. **best-effort**: Sets the best-effort queue. **video**: Sets the video queue. **voice**: Sets the voice queue. **radio** *radio-id*: Indicates that radio of the enabled/disabled 802.11p QoS mapping policy mechanism is selected. Value range: 1-48. This parameter is not available on the fat AP. Only the AC supports configuration of this parameter. **no**: Restores the default settings.
Command Mode	Configure these parameters in AP configuration mode on the fit AP and interface configuration mode on the fat AP.
Usage Guide	The parameter configuration takes effect only when the WMM service is enabled. The 802.1p priority configuration takes effect only when the 802.11p QoS mechanism is enabled.

Enabling DSCP QoS Mapping Policy Mechanism

- Optional configuration.
- Unless otherwise specified, DSCP QoS mapping policy mechanism shall be disabled on all APs.

When the DSCP QoS policy mechanism is enabled, the mapping table related to DSCP QoS is used. When the DSCP QoS policy mechanism is disabled, the default mode is adopted for mapping.

Command	**wmm dscp enable radio** *radio-id*
Parameter Description	**radio** *radio-id*: Indicates that radio of the enabled/disabled DSCP QoS mapping policy mechanism is selected. Value range: 1-48. This parameter is not available on the fat AP. Only the AC supports configuration of this parameter. **no**: Restores the default settings.
Defaults	
Command Mode	Configure these parameters in AP configuration mode on the fit AP and interface configuration mode on the fat AP.
Usage Guide	The parameter configuration takes effect only when the WMM service is enabled.

Configuring How to Apply the DSCP QoS Mapping Policy Mechanism for the AP

- Optional configuration.
- Unless otherwise specified, the DSCP QoS mapping policy mechanism application shall be performed on all APs.

Determine where shall the DSCP domain priority be obtained based on the configuration determining how the AP applies the DSCP QoS mapping policy mechanism.

Command	**wmm dscp policy outer-tunnel** [*outer-tunnel-value*] **inner-tunnel** [*inner-tunnel-value*] **radio** *radio-id*
Parameter Description	**outer-tunnel** *outer-tunnel-value*: Sets how to apply the DSCP QoS mapping policy mechanism for the outer tunnel header. Value range: 0-1. The default is **0**. **Inner-tunnel** *inner-tunnel-value*: Sets how to apply the DSCP QoS mapping policy mechanism for the inner tunnel header. Value range: 0-1. The default is **0**. **radio** *radio-id*: Indicates how the AP applies radio of DSCP QoS mapping policy mechanism. Value range: 1-48. This parameter is not available on the fat AP. Only the AC supports configuration of this parameter.

	no: Restores the default settings.
Command Mode	Configure these parameters in AP configuration mode on the fit AP and interface configuration mode on the fat AP.
Usage Guide	The parameter configuration takes effect only when the WMM service is enabled. The configuration for applying the DSCP QoS mapping policy mechanism takes effect only when the DSCP QoS mechanism is enabled.

Configuring DSCP Identification

- Optional configuration.
- Unless otherwise specified, DSCP identifications shall be configured on all APs.

Determine the DSCP priority based on the configured DSCP identifications.

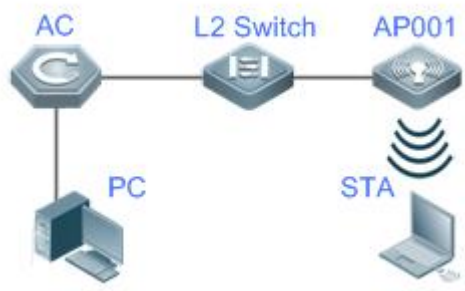
Command	**wmm dscp tag** [*tag-value*] { **back-ground** | **best-effort** | **video** | **voice** } **radio** *radio-id*
Parameter Description	**tag** *tag-value*: Sets the DSCP priority. Value range: 0-63. The default **best-effort** is **0**; the default **back-ground** is **16**; the default **video** is **32**; the default **voice** is **48**. **back-ground**: Sets the back-ground queue. **best-effort**: Sets the best-effort queue. **video**: Sets the video queue. **voice**: Sets the voice queue. **radio** *radio-id*: Sets radio of the DSCP identifications. Value range: 1-48. This parameter is not available on the fat AP. Only the AC supports configuration of this parameter. **no**: Restores the default settings.
Command Mode	Configure these parameters in AP configuration mode on the fit AP and interface configuration mode on the fat AP.
Usage Guide	The parameter configuration takes effect only when the WMM service is enabled. DSCP identification configuration takes effect only when the DSCP mechanism is enabled.

Verification

- You can run the **show run** command on the fat AP or the **show run**/**show ap-config run** command on the fit AP to display the mapping configuration information. When the default configuration is adopted, no configuration information is displayed in the command output.
- Capture packets to check whether the priority mapping is correct.

Configuration Example

Configuring the QoS Packet Priority Mapping

Scenario	
	Connect the AC to the L2 switch, and connect AP001 to the AC through the L2 switch. Configure WLAN1 on AP001. Connect STA to AP001 in wireless mode, and connect the PC to the AC in wired mode.
Configuration Steps	Perform the following configuration on the AC: ● Enter the specified WLAN configuration mode. ● Configure the packet priority mapping.
	FS# configure terminal FS(config)# wlan-config 1 FS(config-wlan)#wlan-qos map-table dot11e-tunnel-dscp import 7 export 50 FS(config-wlan)# end
Verification	Import AC_VO priority traffic in the direction from the STA to PC by using IxChariot, capture packets on the air interface, and display the priority at the wireless end. Then, capture packets from the AC to PC using a packet capturing tool to display the priority at the wired end.

Common Errors

- The WMM service is disabled.

2.5 Monitoring

Debugging

Outputting debugging information consumes system resources. Disable the debugging function immediately after using it.

Command	Function
debug wlan-qos-vsp	Debugs WMM VSP.
debug wlan-qos-cli	Debugs WMM CLI.
debug wlan-qos-map	Debugs WMM mapping.

Chapter 13 WLAN RF Configuration

1. Configuring Band Select

1 Configuring WLAN Optimization

1.1 Overview

Wireless network optimization is to optimize the wireless network and enhance the experience of wireless users by adjusting some configuration of the WLAN.

WLAN configuration can be optimized to:

- Reduce co-channel interference and adjacent-channel interference and enhance signal coverage.
- Increase the channel bandwidth.
- Improve the channel utilization rate.
- Improve the available channel bandwidth for wireless users.
- Decrease network attacks and multicast packet bandwidth usage.
- Improve the downlink throughput of the AP.
- Reduce weak-signal terminals and overall wireless network performance.
- Reduce the influence of the power-saving network adapter.
- Limit the number of access users.

Different WLAN optimization methods are applicable to different application scenarios. See the following table.

WLAN Optimization Method	Application Scenario
Channel planning and adjustment	This method is used as required.
Power planning and adjustment	This method is used as required.
Terminating low-rate applications	This method is applicable to the high-density deployment scenario (school and building).
Establishing a pure 11n wireless network	Settings shall be performed based on actual network requirements.
Adjusting Beacon sending interval	This method is applicable to the high-density deployment scenario where many service set identifiers (SSIDs) are configured for the AP.
Enabling layer 2 isolation for wireless users in a VLAN	This function must be configured for the network not requiring layer 2 mutual-access.
Enabling the RTS/CTS protection mechanism	This method is applicable to the network involving indoor coverage.
Enhancing the AP's packet sending priority and suppressing packet sending by the wireless client	It is recommended that you determine whether to use this method based on actual effects.
Reducing the influence of weak-signal terminals	This method is applicable to the high-density deployment scenario (school and building).
Band selection	This method is applicable to the high-density deployment scenario where the AP supports dual bands.
Power-saving client processing optimization	This method is applicable to all scenarios.
11N A-MPDU aggregation frame sending protection	This method is applicable to all scenarios.
Limiting the STA number on the AP	This method is applicable to the high-density deployment scenario (school and building) with lots of wireless users.

Protocol Specification

- IEEE Std 802.11-2012: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

1.2 Applications

Typical Application	Scenario
802.11n	AP and STA both support the 11n network.
WLAN Spectrum Navigation of Fit AP	Fit AP architecture. The spectrum navigation function is enabled for the WLAN composed of multiple dual-band APs.

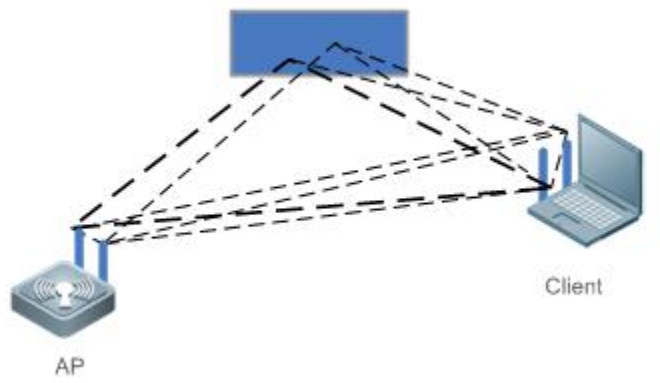
1.2.1 802.11n

Scenario

As a new protocol of the 802.11 protocol family, 802.11n supports two frequency bands, that is, 2.4 GHz and 5 GHz. It aims to provide WLAN access users with higher access rate. 802.11n improves the communication rate by using the MIMO technology or by increasing the bandwidth and improving the channel utilization rate.

As shown in Figure 1-1, the client accesses the wired network through the AP; the client and AP communicate with each other in wireless mode; and there are multiple transmission paths between the client and AP.

Figure 1- 1



Remarks	AP represents a wireless access point. Client represents a wireless client.

Deployment

- Enable the IEEE802.11 protocol on the AP and Client to implement access and authentication of the wireless client.

1.2.2 Spectrum Navigation for WLAN Composed of Fit APs

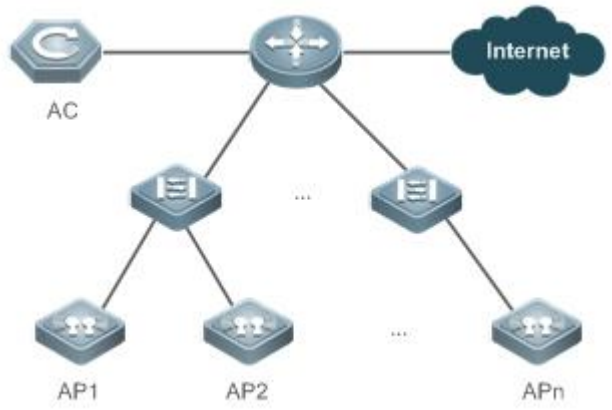
Scenario

Fit AP architecture. The spectrum navigation function is enabled for the WLAN composed of multiple dual-band APs.

As shown in Figure 1- 2:

- One AC is associated with many dual-band APs. The AC and APs are connected by the layer 2 switching device and layer 3 routing device.
- WLAN is mapped to the two radio frequency (RF) interfaces of all dual-band APs.

Figure 1- 2



Remarks	AC represents a wireless access controller. AP1, AP2… and APn are all dual-band APs.

Deployment

- Manage the operating parameters of the spectrum navigation function on the AC device.
- Enable the spectrum navigation function on the AP device to identify the STA type and guide STA access.

1.3 Features

Basic Concepts

WLAN

Wireless Local Area Network (WLAN) interconnects computer devices by using the wireless communication technology to form a network system that supports mutual communication and resource sharing. The essential feature of WLAN is to connect computers to the Internet in wireless mode rather than by using communication cables, facilitating network construction and terminal migration.

AP

Access Point (AP): AP is used for a wireless terminal to access the wired network. It serves as the communication bridge between a wireless terminal and wired network.

STA

Wireless user: A user who accesses the Internet by using a wireless terminal.

RSSI

Received Signal Strength Indication (RSSI) is used to indicate the quality of a wireless link.

Overview

Function and Feature	Description
Terminating Low-Rate Applications	Terminate low-rate applications by configuring the rate set.
Increasing the Beacon Frame Period Appropriately	Lengthen the Beacon frame period; reduce the frequency of sending Beacon frames; reduce the channel usage for packet management; increase the available channel bandwidth for wireless users.
Configuring Layer 2 Isolation of Wireless Users in a VLAN	Configure this function for the network not requiring layer 2 mutual-access to decrease network attacks and multicast packet bandwidth usage.
Configuring Rate Limit for Wireless Users	Make limited network resources serve more users.
Improving the Anti-Interference Capability	When there is co-channel interference, decrease the RTS threshold appropriately to improve the anti-interference capability.
Improving the Capability of Competing for Channels	Adjust the values of the EDCA parameters on the client or AP based on actual requirements to make the AC with a higher priority to start the backoff process earlier than other ACs and preferentially access the channel.
Reducing Weak-Signal Terminals	To control the network coverage of the AP and improve the transmission quality of wireless signals, limit the number of wireless access users.
Limiting the STA Access Number for an AP	Limit the STA number on the AP to implement load balancing to a certain extent, avoiding uneven distribution of AP access users.
Establishing a Pure 11n Network	Configure a pure 11n network to prohibit access of non-11n devices; make all the 11n devices to use pure HT header for transmission; reduce the size of the packet header; increase the available channel bandwidth for the wireless users.
Spectrum Navigation	Guide access of the dual-band STA to the 5G frequency band that has stronger access capacity by means of band selection to reduce the pressure of the 2.4G frequency band, thereby improving user experience.
One-Click Network Optimizaion	After the wireless network runs for a period of time, the following problems may occur: The network speed is slow. Signal or interference problems exist. The authentication page cannot be displayed. STAs equipped with 2.4 GHz/5 GHz network cards are usually associated the network at the 2.4 GHz band. A large number of low-rate packets exist. Multicast packets are lost or re-transmitted. In this case, network optimization is required.

1.3.1 Terminating Low-Rate Applications

Working Principle

Terminate low-rate applications by configuring the rate set.

1.3.2 Relevant Configuration

Configuring the 11a Rate Set

By default, configuration of rates 6 Mbps, 12 Mbps, and 24 Mbps is mandatory, and configuration of rates 9 Mbps, 18 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps is optional.

You can run the **802.11a network rate** command to configure the 11a rate set.

If you disable a rate, this rate can no longer be used. If you disable all rates, 11a wireless users cannot access the WLAN.

Configuring the 11b Rate Set

By default, configuration of rates 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps is mandatory.

You can run the **802.11b network rate** command to configure the 11b rate set.

If you disable a rate, this rate can no longer be used. If you disable all rates, 11b wireless users cannot access the WLAN.

Configuring the 11g Rate Set

By default, configuration of rates 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps is mandatory, and configuration of rates 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps is optional.

You can run the **802.11g network rate** command to configure the 11g rate set.

If you disable a rate, this rate can no longer be used. If you disable all 11b rates, 11b wireless users cannot access the WLAN. If you disable all rates, 11g wireless users cannot access the WLAN.

1.3.3 Increasing the Beacon Frame Period Appropriately

Working Principle

Lengthen the Beacon frame period; reduce the frequency of sending Beacon frames; reduce the channel usage for packet management; increase the available channel bandwidth for wireless users.

Relevant Configuration

➘ Configuring the Beacon Frame Period

By default, the Beacon frame period is 100 milliseconds.

You can run the **beacon period** command to configure the Beacon frame period.

The smaller Beacon period, the more frequently Beacon frames are sent and the more quickly wireless users find the wireless network. However, more Beacon frames require higher channel usage for packet management, reducing the available channel bandwidth for wireless users. If Beacon frame period is set to too great, users may get disconnected from the WLAN or detect the WLAN frequently.

1.3.4 Configuring Layer 2 Isolation of Wireless Users in a VLAN

Working Principle

Configure this function for the network not requiring layer 2 mutual-access to decrease network attacks and multicast packet bandwidth usage.

Relevant Configuration

➘ Configuring WLAN-Based User Isolation for an AP

By default, WLAN-based user isolation is disabled for the AP.

You can run the **user-isolation ssid-ap enable** command to configure WLAN-based user isolation for an AP.

If WLAN-based user isolation is enabled for an AP, wireless users of the same WLAN on this AP cannot access each other at layer 2.

Configuring User Isolation for an AP

By default, user isolation is disabled for the AP.

You can run the **user-isolation ap enable** command to configure user isolation for an AP.

If user isolation is enabled for an AP, wireless users on this AP cannot access each other at layer 2.

Configuring WLAN-Based User Isolation for an AC

By default, WLAN-based user isolation is disabled for the AC.

You can run the **user-isolation ssid-ac enable** command to configure WLAN-based user isolation for an AC.

If WLAN-based user isolation is enabled for an AC, wireless users of the same WLAN on this AC cannot access each other at layer 2.

Configuring User Isolation for an AC

By default, user isolation is disabled for the AC.

You can run the **user-isolation ac enable** command to configure user isolation for an AC.

If user isolation is enabled for an AC, wireless users on this AC cannot access each other at layer 2.

1.3.5 Configuring Rate Limit for Wireless Users

Working Principle

To make limited network resources serve more users, ensure that the device supports the traffic rate limit function. When the data traffic accords with the committed rate, data packets are allowed to pass. When the data traffic does not accord with the committed rate, data packets are discarded.

Relevant Configuration

Configuring AP-Based Rate Limit

By default, AP-based rate limit is disabled.

You can run the **ap-based** command to configure the AP-based rate limit.

The greater the rate is, the greater the transmission rate available for the STA is.

Configuring Client-Based Rate Limit

By default, client-based rate limit is disabled.

You can run the **netuser** command to configure the client-based rate limit.

The greater the rate is, the greater the transmission rate available for the STA is.

Configuring WLAN-Based Rate Limit

By default, WLAN-based rate limit is disabled.

You can run the **wlan-based** command to configure the WLAN-based rate limit.

The greater the rate is, the greater the transmission rate available for the STA is.

1.3.6 Improving the Anti-Interference Capability

Working Principle

To avoid data transmission failure caused by conflicts between channels, the IEEE 802.11 MAC protocol provides a Request to Send/Clear to Send (RTS/CTS) handshake protocol, that is, requests to send/allow sending protocol. The following description assumes that workstation A needs to send data to workstation B. First of all, workstation A sends a RTS request frame. If workstation B allows workstation A to send the request frame, workstation B replies a CTS permission frame. After receiving this permission frame, workstation A begins to sending data. If multiple workstations send RTS requests to the same workstation, only the workstations receiving CTS are allowed to send data. For the workstation not receiving CTS, it is regarded that channel conflict occurs. In this case, this workstation waits for a certain time and sends a RTS request again.

If RTS/CTS handshake needs to be performed when a workstation sends data each time, excessive RTS frames will occupy much channel bandwidth. Users can set the RTS threshold to specify the length of the data frame to be sent. RTS/CTS handshake is not performed when a workstation sends a data frame with a length smaller than the RTS threshold.

Relevant Configuration

↘ Configuring the RTS Threshold

By default, the RTS threshold is 2347 bytes.

You can run the **rts threshold** command to set the RTS threshold.

When co-channel interference exists, a smaller RTS threshold means a higher anti-interference capability. However, more RTS/CTS packets require greater channel usage for packet control, reducing the available channel bandwidth for wireless users.

1.3.7 Improving the Capability of Competing for Channels

Working Principle

EDCA parameters differentiate access capabilities of channels with different priorities. Each AC has its own EDCA channel competition parameters. Users can adjust the values of the EDCA parameters on the client or AP based on actual requirements to make the AC with a higher priority to start the backoff process earlier than other ACs and preferentially access the channel.

During actual configuration, you can choose to configure the EDCA parameters on the client or side based on application requirements. Configuration of EDCA parameters on the client and AP respectively affects the downlink data traffic and uplink data traffic.

Relevant Configuration

↘ Configuring the EDCA Parameters on the Client

By default, the EDCA parameters on the client are as follows:

You can run the **wmm edca-client** command to configure the EDCA parameters on the client.

The smaller AIFS is, the earlier the backoff process starts and the stronger the channel access capability is. Smaller CWmin and CWmax mean shorter backoff time determined by CWmin and CWmax, earlier termination of the backoff process, and stronger channel access capability. Larger TXOP limit means that more packets are to be transmitted continuously by using the SIFS interval after preempting the transmission chance. The packet conflict probability and waste of air interface resources can be reduced to a certain extent by increasing the TXOP limit.

Configuring the EDCA Parameters on the AP

By default, the EDCA parameters on the AP are as follows:

You can run the **wmm edca-radio** command to configure the EDCA parameters on the AP.

The smaller AIFS is, the earlier the backoff process starts and the stronger the channel access capability is. Smaller CWmin and CWmax mean shorter backoff time determined by CWmin and CWmax, earlier termination of the backoff process, and stronger channel access capability. Larger TXOP limit means that more packets are to be transmitted continuously by using the SIFS interval after preempting the transmission chance. The packet conflict probability and waste of air interface resources can be reduced to a certain extent by increasing the TXOP limit.

1.3.8 Reducing Weak-Signal Terminals

Working Principle

Wireless users search for the AP in active scanning or passive scanning mode.

- Active scanning: A wireless user sends a Probe Request for accessing the AP. After confirming the request frame, the AP returns a Probe Response frame.
- Passive scanning: The AP periodically broadcasts Beacon frames. A wireless user attempts to connect to the AP after listening Beacon frames.

To control the network coverage of the AP and improve the transmission quality of wireless signals, limit the number of wireless access users. You can control the Beacon frame broadcast coverage of the AP to prevent access of remote wireless users. You can also limit the minimum value of the RSSI for wireless users. When the RSSI of the request frame sent from a wireless user is smaller than this minimum value, the access of this wireless user is not allowed.

Relevant Configuration

Configuring the Minimum RSSI for Wireless User Access

By default, the minimum RSSI for wireless user access is 0. That is, all users are allowed to access the WLAN, no matter how large the RSSI is.

You can run the **response-rssi** command to set the minimum RSSI for wireless user access.

A smaller minimum RSSI means that wireless users farther from the FAT-AP are allowed to access the WLAN.

Configuring the Management Frame Transmit Power

By default, the management frame transmit power is 0. That is, the management frame transmit power is not configured by default.

You can run the **coverage-area-control** command to set the management frame transmit power.

A larger management frame transmit power (excluding 0) means a larger wireless-user coverage of the FAT-AP, indicating that wireless users farther from the FAT-AP are allowed to access the WLAN.

Limiting the STA Number for an AP

Working Principle

In a WLAN, one AP allows access of multiple wireless users, and the administrator can specify the maximum number of wireless users. Limit the STA access number for the AP to implement load balancing to a certain extent, avoiding uneven distribution of AP access users.

Relevant Configuration

Configuring AP-Based STA Number Limit

By default, the AP-based STA number limit is 32.

You can run the **sta-limit** command to configure the AP-based STA number limit.

A larger AP-based STA number limit means that more STAs are allowed to access the WLAN.

1.3.9 Establishing a Pure 11n Network

Working Principle

Configure a pure 11n network to prohibit access of non-11n devices; make all the 11n devices of the network to use pure HT header for transmission; reduce the size of the packet header; increase the available channel bandwidth for the wireless users.

Relevant Configuration

Configuring Whether to Support 11a or Not

By default, STA access of 11a is supported.

You can run the **11asupport enable** command to configure whether to support 11a or not.

If 11a is supported, STA access of 11a is allowed. Otherwise, STA access of 11a is prohibited.

Configuring Whether to Support 11b or Not

By default, STA access of 11b is supported.

You can run the **11bsupport enable** command to configure whether to support 11b or not.

If 11b is supported, STA access of 11b is allowed. Otherwise, STA access of 11b is prohibited.

Configuring Whether to Support 11g or Not

By default, STA access of 11g is supported.

You can run the **11gsupport enable** command to configure whether to support 11g or not.

If 11g is supported, STA access of 11g is allowed. Otherwise, STA access of 11g is prohibited.

Configuring Whether to Support 11n or Not at 5 GHz

By default, STA access of 11n at 5 GHz is supported.

You can run the **11nasupport enable** command to configure whether to support 11n or not at 5 GHz.

If 11n is supported at 5 GHz, STA access of 11n at 5 GHz is allowed. Otherwise, STA access of 11n at 5 GHz is prohibited.

Configuring Whether to Support 11n or Not at 2.4 GHz

By default, STA access of 11n at 2.4 GHz is supported.

You can run the **11ngsupport enable** command to configure whether to support 11n or not at 2.4 GHz.

If 11n is supported at 2.4 GHz, STA access of 11n at 2.4 GHz is allowed. Otherwise, STA access of 11n at 2.4 GHz is prohibited.

1.3.10 Spectrum Navigation

Working Principle

IEEE802.11 mainly has two communication frequency bands:

- 2.4 GHz (2.412 to 2.4835 GHz) (IEEE 802.11b/g operates in this frequency range)
- 5 GHz (5.15 to 5.35 and 5.725 to 5.825 GHz) (IEEE 802.11a operates in this frequency range)

Dual-band STA supports both 2.4G and 5G frequency bands. However, users lack professional knowledge; most wireless access service vendors do not provide effective guidance; 802.11b/g is more widely applied than 802.11a. Consequently, many dual-band STAs only use the 2.4G frequency band, causing congestion of the 2.4G frequency band and waste of the 5G frequency band. In fact, the 5G frequency band has a stronger access capacity than the 2.4G frequency band: The 2.4G frequency band at most has three non-overlapping communication channels, whereas the 5G frequency band can provide more than three non-overlapping communication channels. For example, 13 in China and up to 24 in North America.

Guide access of the dual-band STA to the 5G frequency band that has stronger access capacity by means of band selection to reduce the pressure of the 2.4G frequency band, thereby improving user experience.

Relevant Configuration

Lower Limit of STA Signal Strength Accepted by Spectrum Navigation

By default, the lower limit of STA signal strength accepted by spectrum navigation is -80 dBm.

You can run the **band-select acceptable-rssi** command to set the lower limit of STA signal strength accepted by spectrum navigation. The range is from -100 to -50.

A larger lower limit means a smaller coverage of the spectrum navigation. That is, a smaller lower limit means a larger coverage of the spectrum navigation. However, if the lower limit exceeds the limit for normal use, the access STA signal will be very weak, reducing the connection rate of the entire network.

STA Information Aging Time

By default, the aging time of dual-band STA information is 60 seconds, and the aging time of suppression STA information is 20 seconds.

You can run the **band-select age-out** command to adjust the aging time of STA information. The aging time of dual-band STA information ranges from 20 to 120 seconds, and the aging time of suppression STA information ranges from 10 to 60 seconds.

The longer STA information aging time is, the longer STA information lifecycle is, indicating that the AP is more insensitive to switching of STA frequency bands. The shorter STA information aging time is, the shorter STA information lifecycle is, indicating that the AP is more sensitive to switching of STA frequency bands.

1.3.11 One-Click Network Optimization

Working Principle

After the wireless network runs for a period of time, the following problems may occur:

The network speed is slow.

Signal or interference problems exist.

The authentication page cannot be displayed.

STAs equipped with 2.4 GHz/5 GHz network cards are usually associated the network at the 2.4 GHz band.

A large number of low-rate packets exist.

Multicast packets are lost or re-transmitted.

In this case, network optimization is required.

1. The network speed is slow.

The possible causes are as follows:

No rate limit is configured. Some users occupy large bandwidth for downloading or playing videos. As a result, the network speed of other users is slow.

A rate limit is configured but the rate is high, without achieving the rate limit effect.

A rate limit is configured but the rate is low, resulting in slow network speed.

For this problem, the rate limit solution can be used. Rate limiting is performed for all STAs by WLAN to ensure that the average uplink and downlink rate is 256 kbit/s and the abrupt rate is 300 kbit/s.

2. Signal or interference problems exist.

For example, the signal is poor, roaming frequently occurs, or intra-frequency/inter-frequency interference occurs. For this problem, the RRM function can be used. After the RRM function is enabled, channel or power adjustment is performed for online APs or newly added APs to ensure signal coverage and channel different from those of neighboring APs. If the poor signal or intra-frequency/inter-frequency interference problem does not exist, disable the RRM function to improve the device performance.

3. The authentication page cannot be displayed.

This is because few sessions are configured. For this problem, restore the default number of sessions to ensure that each STA supports 255 sessions and each port supports 1000 sessions by default.

4. STAs equipped with 2.4 GHz/5 GHz network cards are usually associated the network at the 2.4 GHz band.

For this problem, the 5 GHz preferred function can be used. If only few STAs supporting 5 GHz exist in the environment, it is recommended that the 5 GHz preferred function be disabled.

5. A large number of low-rate packets exist.

For this problem, the low-rate packet forbidding function can be used to forbid packets complying with 802.11b, 802.11g, or 802.11a and with a rate lower than 11 Mbps.

6. Multicast packets are lost or re-transmitted.

This is because a high multicast rate is set. For this problem, restore the default multicast rate to ensure user experience.

1.3.12 Intelligent Network Optimization

Perform wireless network optimization intelligently.

Working Principle

Perform wireless network optimization intelligently based on real-time network running.

1.3.13 Mcell Configuration

Enable dense deployment optimization.

Working Principle

Enable dense deployment optimization.

1.3.14 Roaming Stickiness

Working Principle

Monitor terminals with low RSSI and poor user experience on the entire wireless network in real time and determine whether more suitable APs exist for terminals to access the network based on the terminal detection information collected by each AP. If such terminals with sticky roaming exist, the AP sends a deauthentication frame to disassociate with the terminal to ensure that the terminal is associated with an AP with better signal quality.

1.3.15 Remote Association Information Collection

Working Principle

Determine whether a terminal is associated with the AP with the optimal signal quality based on the terminal detection information. If it is detected that a terminal associates with an AP with poor signal quality, a notification is reported to the WIS client. Based on collected remote association information, the WIS client performs coverage optimization for APs.

1.3.16 Automatic Device Information Upload

Working Principle

Configure automatic upload of the AC and AP software and hardware version numbers.

1.4 Configuration

Configuration Item	Configuration Suggestion & Relevant Command	
Configuring the Rate Set	Optional. It is used to terminate low-rate applications.	
	802.11a network rate	Configures the 11a rate set.
	802.11b network rate	Configures the 11b rate set.
	802.11g network rate	Configures the 11g rate set.
Configuring the Beacon Frame Period	Optional. It is used to increase the Beacon frame period.	
	beacon period	Configures the Beacon frame period.
Configuring Layer 2 Isolation of Wireless Users in a VLAN	Optional. It is used to enable layer 2 isolation of wireless users in a VLAN.	
	user-isolation ssid_ap enable	Configures WLAN-based user isolation for an AP.
	user-isolation ap enable	Configures user isolation for an AP.
	user-isolation ssid_ac enable	Configures WLAN-based user isolation for an AC.
	user-isolation ac enable	Configures user isolation for an AC.
Configuring Rate Limit for	Optional. It is used to configure rate limit for wireless users.	

Wireless Users	**ap-based**	Configures AP-based rate limit.
	netuser	Configures client-based rate limit.
	wlan-based	Configures WLAN-based rate limit.
Configuring the RTS/CTS Protection Mechanism	Optional. It is used to configure the RTS/CTS protection mechanism.	
	rts-threshold	Configures the RTS threshold.
Configuring EDCA Parameters	Optional. It is used to configure EDCA parameters.	
	wmm edca-client	Configures the EDCA parameters on the client.
	wmm edca-radio	Configures the EDCA parameters on the AP.
Configuring the Allowed Access Signal Strength	Optional. It is used to configure the allowed access signal strength.	
	response-rssi	Configures the minimum RSSI for wireless user access.
	coverage-area-control	Configures the management frame transmit power.
Configuring the Number of Access Users Allowed by the AP	Optional. It is used to configure the number of access users allowed by the AP.	
	sta-limit	Configures AP-based STA number limit.
Configuring a Pure 11n Network	Optional. It is used to configure a pure 11n network.	
	11asupport	Configures whether to support 11a or not.
	11bsupport	Configures whether to support 11b or not.
	11gsupport	Configures whether to support 11g or not.
	11nasupport	Configures whether to support 11na or not.
	11ngsupport	Configures whether to support 11ng or not.
Configuring Spectrum Navigation	Mandatory. It is used to enable the spectrum navigation function of the WLAN.	
	band-select enable	Enables the spectrum navigation function.
	Optional. It is used to configure the operating parameters of the spectrum navigation function.	
	band-select acceptable-rssi	Configures the lower limit of STA signal strength accepted by spectrum navigation.
	band-select access-denial	Configures the number of times for which dual-band STA access to 2.4G band is denied.
	band-select age-out	Configures the STA information aging time.
	band-select probe-count	Configures the detection period count of suppression STA.
	band-select scan-cycle	Configures the threshold of STA detection scanning period.
Configuring One-Click	Optional. It is used to configure network optimization options.	

Network Optimization	**wopt choose**	Configures network optimization options.
	Optional. It is used to configure one-click network optimization.	
	wopt enable	Configures one-click network optimization.
Configuring Intelligent Network Optimization	Optional. It is used to configure network optimization options.	
	wis enable	Enables intelligent network optimization.
Configuring mcell	Optional. It is used to configure network optimization options.	
	mcell enable	Enables dense deployment optimization.
Configuring Roaming Stickness	Optional. It is used to configure network optimization options.	
	sticky-steering monitor-only	Enables roaming stickiness monitoring.
	Optional. It is used to configure one-click network optimization.	
	sticky-steering enable	Enables roaming stickiness navigation.
Configuring Remote Association	Optional. It is used to configure network optimization options.	
	farpoint-steering enable	Enables remote association.

1.4.1 Configuring the Rate Set

Configuration Effect

- Configure the rate set to terminate low-rate applications; prohibit packet transmission at low rate between the STA and AP; improve the channel usage.

Notes

- If you disable a rate, this rate can no longer be used.
- If you disable all rates, wireless users cannot access the WLAN.
- If you disable all 11b rates, 11b wireless users cannot access the WLAN.

Configuration Steps

Configuring the 11a Rate Set

- Mandatory configuration. By default, configuration of rates 6 Mbps, 12 Mbps, and 24 Mbps is mandatory, and configuration of rates 9 Mbps, 18 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps is optional.
- Unless otherwise specified, the configuration shall be performed in AC configuration mode on the AC device.

Configuring the 11b Rate Set

- Optional configuration. By default, configuration of rates 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps is mandatory.
- Unless otherwise specified, the configuration shall be performed in AC configuration mode on the AC device.

Configuring the 11g Rate Set

- Optional Configuration. By default, configuration of rates 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps is mandatory, and configuration of rates 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps is optional.
- Unless otherwise specified, the configuration shall be performed in AC configuration mode on the AC device.

Verification

- You can run the **show running** command to display the configuration information of the rate set.

Related Commands

Configuring the 11a Rate Set

Command	**802.11a network rate** { **6** | **9** | **12** | **18** | **24** | **36** | **48** | **54** } { **disable** | **mandatory** | **supported** }
Parameter Description	**6**: The rate is 6 Mbps. **9**: The rate is 9 Mbps. **12**: The rate is 12 Mbps. **18**: The rate is 18 Mbps. **24**: The rate is 24 Mbps. **36**: The rate is 36 Mbps. **48**: The rate is 48 Mbps. **54**: The rate is 54 Mbps. **disable**: Disables the rate. **mandatory**: Specifies the mandatory rate. **supported**: Specifies the supported rate.
Command Mode	AC configuration mode
Defaults	N/A
Usage Guide	N/A

Configuring the 11b Rate Set

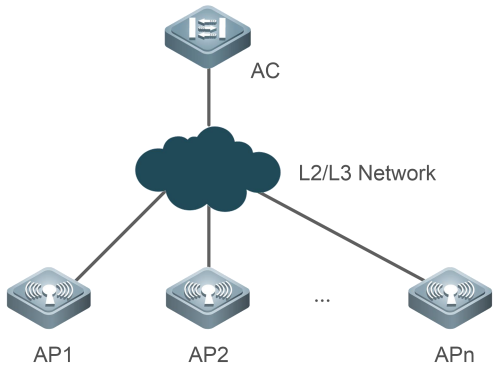
Command	**802.11b network rate** { **1** | **2** | **5** | **11** } { **disable** | **mandatory** | **supported** }
Parameter Description	**1**: The rate is 1 Mbps. **2**: The rate is 2 Mbps. **5**: The rate is 5.5 Mbps. **11**: The rate is 11 Mbps. **disable**: Disables the rate. **mandatory**: Specifies the mandatory rate. **supported**: Specifies the supported rate.
Command Mode	AC configuration mode
Defaults	N/A
Usage Guide	N/A

Configuring the 11g Rate Set

Command	**802.11g network rate** { **1** | **2** | **5** | **6** | **9** | **11** | **12** | **18** | **24** | **36** | **48** | **54** } { **disable** | **mandatory** | **supported** }
Parameter Description	**1**: The rate is 1 Mbps. **2**: The rate is 2 Mbps. **5**: The rate is 5.5 Mbps. **6**: The rate is 6 Mbps. **9**: The rate is 9 Mbps. **11**: The rate is 11 Mbps. **12**: The rate is 12 Mbps. **18**: The rate is 18 Mbps. **24**: The rate is 24 Mbps. **36**: The rate is 36 Mbps. **48**: The rate is 48 Mbps. **54**: The rate is 54 Mbps. **disable**: Disables the rate. **mandatory**: Specifies the mandatory rate. **supported**: Specifies the supported rate.
Command Mode	AC configuration mode
Defaults	N/A
Usage Guide	N/A

Configuration Examples

Configuring the Rate Set

Scenario **Figure 1-3**	
Configuration Steps	● Disable the 6 Mbps rate for 802.11a users on the AC device. ● Disable the 1 Mbps and 2 Mbps rates for the 802.11b users on the AC device. ● Disable the 1 Mbps, 2 Mbps, and 5.5 Mbps rates for 802.11g users on the AC device.
AC	FS#configure terminal FS(config)#ac-controller FS(config-ac)#802.11a network rate 6 disabled FS(config-ac)#802.11b network rate 1 disabled FS(config-ac)#802.11b network rate 2 disabled

	FS(config-ac)#802.11g network rate 1 disabled FS(config-ac)#802.11g network rate 2 disabled FS(config-ac)#802.11g network rate 5 disabled
Verification	After configuring the rate set, you can display the configuration information of the rate set for a check. ● You can run the **show running** command to display the configuration information of the rate set.
	FS#show running ! ac-controller country CN country US 802.11g network rate 1 disabled 802.11g network rate 2 disabled 802.11g network rate 5 disabled 802.11g network rate 11 mandatory 802.11g network rate 6 supported 802.11g network rate 9 supported 802.11g network rate 12 supported 802.11g network rate 18 supported 802.11g network rate 24 supported 802.11g network rate 36 supported 802.11g network rate 48 supported 802.11g network rate 54 supported 802.11b network rate 1 disabled 802.11b network rate 2 disabled 802.11b network rate 5 mandatory 802.11b network rate 11 mandatory 802.11a network rate 6 disabled 802.11a network rate 9 supported 802.11a network rate 12 mandatory 802.11a network rate 18 supported 802.11a network rate 24 mandatory 802.11a network rate 36 supported 802.11a network rate 48 supported 802.11a network rate 54 supported !

Common Errors

None.

1.4.2 Configuring the Beacon Frame Period

Configuration Effect

- Lengthen the Beacon frame period; reduce the frequency of sending Beacon frames; reduce the channel usage for packet management; increase the available channel bandwidth for wireless users.

Notes

- If Beacon frame period is set to too great, users may get disconnected from the WLAN or detect the WLAN frequently.

Configuration Steps

Configuring the Beacon Frame Period

- Optional configuration. By default, the Beacon frame period is 100 milliseconds.
- Unless otherwise specified, the configuration shall be performed in AP configuration mode on the AC device.

Verification

- You can run the **show ap-config running** command to display the configuration information of the Beacon frame period.

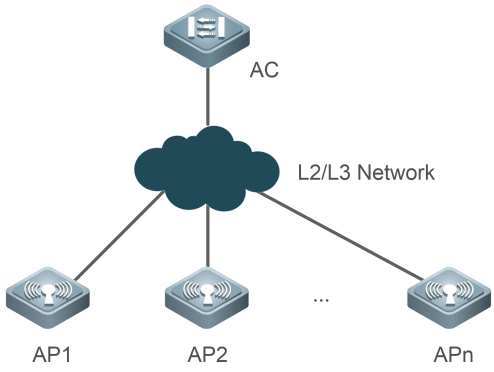
Related Commands

Configuring the Beacon Frame Period

Command	**beacon period** *milliseconds* **radio** *radio-id*
Parameter Description	*milliseconds*: Specifies the Beacon frame period, in the range from 20 to 1,000 in the unit of milliseconds. *radio-id*: Specifies the RF interface index, in the range from 1 to 16.
Command Mode	AP configuration mode
Defaults	100 milliseconds
Usage Guide	Configuration for all APs is not supported.

Configuration Examples

Configuring the Beacon Frame Period

Scenario **Figure 1-4**	
Configuration Steps	● Set the Beacon frame period of AP1 Radio1 to 300 milliseconds on the AC device.
AC	FS#configure terminal

	FS(config)#ap-config AP1 FS(config-ap)#beacon period 300 radio 1
Verification	After configuring the Beacon frame period, you can display the configuration information of the Beacon frame period for a check. ● You can run the **show ap-config running** command to display the configuration information of the Beacon frame period.
	FS#show ap-config running AP1 ! ap-config AP1 no 11acsupport enable radio 1 no 11acsupport enable radio 2 802.11n mcs support 15 radio 1 802.11n mcs support 15 radio 2 antenna receive 3 radio 1 antenna receive 3 radio 2 antenna transmit 3 radio 1 antenna transmit 3 radio 2 radio-type 1 802.11b radio-type 2 802.11a beacon period 300 radio 1 beacon period 100 radio 2 ap-mac 001a.a9c5.3f49 no enable-radio 1 no enable-radio 2 !

Common Errors

None.

1.4.3 Configuring Layer 2 Isolation of Wireless Users in a VLAN

Configuration Effect

- Configure this function for the network not requiring layer 2 mutual-access to decrease network attacks and multicast packet bandwidth usage.

Notes

- None.

Configuration Steps

Configuring WLAN-Based User Isolation for an AP

- Optional configuration. By default, WLAN-based user isolation is disabled for the AP.

- Unless otherwise specified, the configuration shall be performed in WIDS configuration mode on the AC device.

Configuring User Isolation for an AP

- Optional configuration. By default, user isolation is disabled for the AP.
- Unless otherwise specified, the configuration shall be performed in WIDS configuration mode on the AC device.

Configuring WLAN-Based User Isolation for an AC

- Optional configuration. By default, WLAN-based user isolation is disabled for the AC.
- Unless otherwise specified, the configuration shall be performed in WIDS configuration mode on the AC device.

Configuring User Isolation for an AC

- Optional configuration. By default, user isolation is disabled for the AC.
- Unless otherwise specified, the configuration shall be performed in WIDS configuration mode on the AC device.

Verification

- You can run the **show running** command to display the configuration information of layer 2 isolation of wireless users in a VLAN.

Related Commands

Configuring WLAN-Based User Isolation for an AP

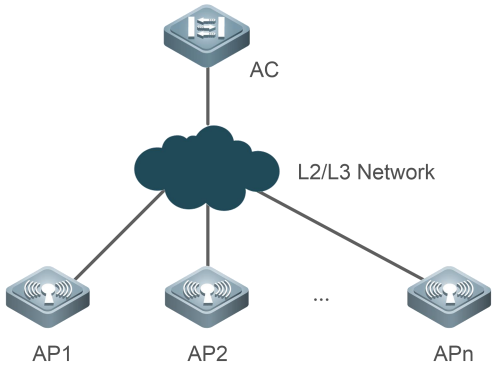
Configuring User Isolation for an AP

Configuring WLAN-Based User Isolation for an AC

Configuring User Isolation for an AC

Configuration Examples

Configuring Layer 2 Isolation of Wireless Users in a VLAN

Scenario Figure 1-5	
Configuration Steps	• Enable WLAN-based user isolation for an AP on the AC device. • Enable user isolation for an AP on the AC device. • Enable WLAN-based user isolation for an AC on the AC device. • Enable user isolation for an AC on the AC device.

AC	FS#configure terminal FS(config)#wids FS(config-wids)#user-isolation ssid-ap enable FS(config-wids)#user-isolation ap enable FS(config-wids)#user-isolation ssid-ac enable FS(config-wids)#user-isolation ac enable
Verification	After configuring layer 2 isolation of wireless users in a VLAN, you can display the configuration information on layer 2 isolation of wireless users in a VLAN for a check. ● You can run the **show running** command to display the configuration information on layer 2 isolation of wireless users in a VLAN.
	FS#show running ! wids user-isolation ap enable user-isolation ac enable user-isolation ssid-ac enable user-isolation ssid-ap enable !

1.4.4 Configuring Rate Limit for Wireless Users

Configuration Effect

- To make limited network resources serve more users, ensure that the device supports the traffic rate limit function. When the data traffic accords with the committed rate, data packets are allowed to pass. When the data traffic does not accord with the committed rate, data packets are discarded.

Notes

- When the data traffic does not accord with the committed rate, data packets are discarded.

Configuration Steps

Configuring AP-Based Rate Limit

- Optional configuration. By default, AP-based rate limit is disabled.
- Unless otherwise specified, the configuration shall be performed in AP configuration mode on the AC device.

Configuring Client-Based Rate Limit

- Optional configuration. By default, client-based rate limit is disabled.
- Unless otherwise specified, the configuration shall be performed in AC configuration mode on the AC device.

Configuring WLAN-Based Rate Limit

- Optional configuration. By default, WLAN-based rate limit is disabled.
- Unless otherwise specified, the configuration shall be performed in WLAN configuration mode on the AC device.

Verification

- You can run the **show running** command to display the configuration information of the rate limit for wireless users.

Related Commands

Configuring AP-Based Rate Limit

Command	**ap-based { per-user-limit | total-user-limit } { up-streams | down-streams } average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*
Parameter Description	**per-user-limit**: Limits the rates of all users on the AP. **total-user-limit**: Limits the rate of the whole AP is limited. **up-streams**: Limits the rate of uplink traffic. **down-streams**: Limits the rate of downlink traffic. *average-data-rate*: Specifies the average rate limit, in the range from 8 to 261120 in the unit of . *burst-data-rate*: Specifies the burst rate limit, in the range from 8 to 261120 in the unit of .
Command Mode	AP configuration mode
Defaults	AP-based rate limit is disabled by default.
Usage Guide	N/A

Configuring Client-Based Rate Limit

Command	**netuser** *mac-address* **{ inbound | outbound } average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*
Parameter Description	*mac-address*: Specifies the MAC address of the user. **inbound**: Limits the rate of uplink traffic. **outbound**: Limits the rate of downlink traffic. *average-data-rate*: Specifies the average rate limit, in the range from 8 to 261120 in the unit of . *burst-data-rate*: Specifies the burst rate limit, in the range from 8 to 261120 in the unit of .
Command Mode	AC configuration mode
Defaults	Client-based rate limit is disabled by default.
Usage Guide	N/A

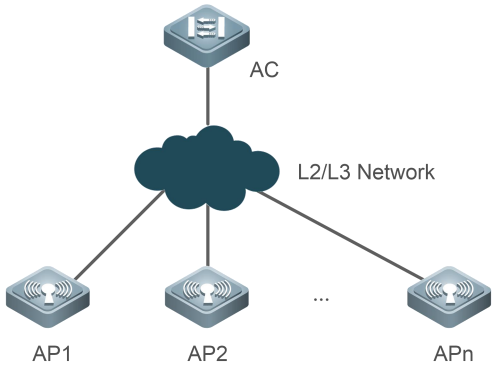
Configuring WLAN-Based Rate Limit

Command	**wlan-based { per-user-limit | total-user-limit | per-ap-limit } { up-streams | down-streams } average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*
Parameter Description	**per-user-limit**: Limits the rates of all users in the WLAN. **total-user-limit**: Limits the rate of the whole WLAN. **per-ap-limit**: Limits the rate of the whole WLAN for each AP separately. **up-streams**: Limits the rate of uplink traffic. **down-streams**: Limits the rate of downlink traffic. *average-data-rate*: Specifies the average rate limit, in the range from 8 to 261120 in the unit of . *burst-data-rate*: Specifies the burst rate limit, in the range from 8 to 261120 in the unit of .

Command Mode	WLAN configuration mode
Defaults	WLAN-based rate limit is disabled by default.
Usage Guide	N/A

Configuration Examples

Configuring Rate Limit for Wireless Users

Scenario **Figure 1-6**	
Configuration Steps	● Limit the maximum uplink average rate and maximum uplink burst rate of each user on AP1 to 256 Kbps and 1024 Kbps respectively on the AC device. ● Limit the maximum uplink average rate and maximum uplink burst rate of wireless user 14cf.920b.bfce on the AC to 256 Kbps and 1024 Kbps respectively on the AC device. ● Limit the maximum uplink average rate and maximum uplink burst rate of each user in WLAN 12 to 256 Kbps and 1024 Kbps respectively on the AC device.
	FS#configure terminal FS(config)#ap-config AP1 FS(config-ap)#ap-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024 FS(config-ap)#end FS#configure terminal FS(config)#ac-controller FS(config-ac)#netuser 14cf.920b.bfce inbound average-data-rate 256 burst-data-rate 1024 FS(config-ap)#end FS#configure terminal FS(config)#wlan-config 12 FS(config-wlan)#wlan-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024
Verification	After configuring the rate limit for wireless users, you can display the configuration information of the rate limit for wireless users for a check. ● You can run the **show running** command to display the configuration information of the rate limit for wireless users.
	FS#show ap-config running AP1 !

```
ap-config AP1
 ap-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024
 no 11acsupport enable radio 1
 no 11acsupport enable radio 2
 802.11n mcs support 15 radio 1
 802.11n mcs support 15 radio 2
 antenna receive 3 radio 1
 antenna receive 3 radio 2
 antenna transmit 3 radio 1
 antenna transmit 3 radio 2
 radio-type 1 802.11b
 radio-type 2 802.11a
 beacon period 300 radio 1
 beacon period 100 radio 2
 ap-mac 001a.a9c5.3f49
 no enable-radio 1
 no enable-radio 2
!
FS#show running
!
wlan-config 12 wlan_opt
 wlan-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024
 enable-broad-ssid
!
!
ac-controller
 netuser 14cf.920b.bfce inbound average-data-rate 256 burst-data-rate 1024
 country CN
 country US
 802.11g network rate 1 disabled
 802.11g network rate 2 disabled
 802.11g network rate 5 disabled
 802.11g network rate 11 mandatory
 802.11g network rate 6 supported
 802.11g network rate 9 supported
 802.11g network rate 12 supported
 802.11g network rate 18 supported
 802.11g network rate 24 supported
 802.11g network rate 36 supported
 802.11g network rate 48 supported
 802.11g network rate 54 supported
 802.11b network rate 1 disabled
 802.11b network rate 2 disabled
 802.11b network rate 5 mandatory
```

	802.11b network rate 11 mandatory 802.11a network rate 6 disabled 802.11a network rate 9 supported 802.11a network rate 12 mandatory 802.11a network rate 18 supported 802.11a network rate 24 mandatory 802.11a network rate 36 supported 802.11a network rate 48 supported 802.11a network rate 54 supported !

Common Errors

None.

1.4.5 Configuring the RTS/CTS Protection Mechanism

Configuration Effect

- When co-channel interference exists, a smaller RTS threshold means a higher anti-interference capability. However, more RTS/CTS packets require higher channel usage for packet control, reducing the available channel bandwidth for wireless users. Users can set the RTS threshold to specify the length of the data frame to be sent. RTS/CTS handshake is not performed when a workstation sends a data frame with a length smaller than the RTS threshold.

Notes

- None.

Configuration Steps

Configuring the RTS Threshold

- Optional configuration. By default, the RTS threshold is 2347 bytes.
- Unless otherwise specified, the configuration shall be performed in AP configuration mode on the AC device.

Verification

- You can run the **show ap-config running** command to display the configuration information of the RTS threshold.

Related Commands

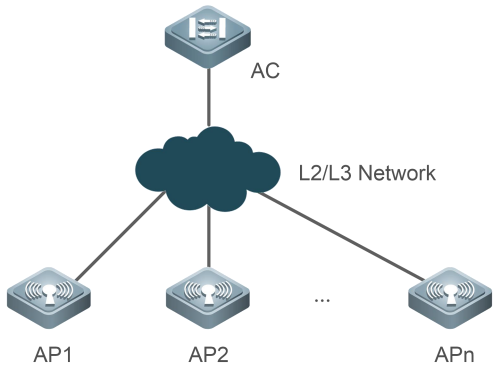
Configuring the RTS Threshold

Command	**rts-threshold** *value* **radio** *radio-id*
Parameter Description	*value*: Specifies the RTS threshold, in the range from 257 to 2,347 in the unit of bytes. *radio-id*: Specifies the RF interface index, in the range from 1 to 48.
Command Mode	AP configuration mode
Defaults	The RTS threshold is 2,347 bytes by default.

Usage Guide	N/A

Configuration Examples

Configuring the RTS Threshold

Scenario **Figure 1-7**	
Configuration Steps	● Set the RTS threshold of AP1 Radio1 to 800 bytes on the AC.
AC	FS#configure terminal FS(config)#ap-config AP1 FS(config-ap)#rts-threshold 800 radio 1
Verification	After configuring the RTS threshold, you can display the configuration information of the RTS threshold for a check. ● You can run the **show ap-config running** command to display the configuration information of the RTS threshold.
	FS#show ap-config running AP1 ! ap-config AP1 ap-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024 no 11acsupport enable radio 1 no 11acsupport enable radio 2 802.11n mcs support 15 radio 1 802.11n mcs support 15 radio 2 rts-threshold 800 radio 1 antenna receive 3 radio 1 antenna receive 3 radio 2 antenna transmit 3 radio 1 antenna transmit 3 radio 2 radio-type 1 802.11b radio-type 2 802.11a beacon period 300 radio 1 beacon period 100 radio 2 ap-mac 001a.a9c5.3f49

	no enable-radio 1 no enable-radio 2 !

Common Errors

None.

1.4.6 Configuring EDCA Parameters

Configuration Effect

- During actual configuration, you can choose to configure the EDCA parameters on the client or AP based on application requirements. Configuration of EDCA parameters on the client and AP respectively affects the downlink data traffic and uplink data traffic.

Notes

- None.

Configuration Steps

Configuring the EDCA Parameters on the Client

- Optional configuration. By default, the EDCA parameters on the client are as follows:
- Unless otherwise specified, the configuration shall be performed in AP configuration mode on the AC device.

Configuring the EDCA Parameters on the AP

- Optional configuration. By default, the EDCA parameters on the AP are as follows:
- Unless otherwise specified, the configuration shall be performed in AP configuration mode on the AC device.

Verification

- You can run the **show ap-config running** command to display the configuration information of the EDCA parameters.

Related Commands

Configuring the EDCA Parameters on the Client Side

Command	**wmm edca-client** { **back-ground** | **best-effort** | **video** | **voice** } { **aifsn** [*aifsn-value*] **cwmin** [*cwmin-value*] **cwmax** [*cwmax-value*] **txop** [*txop-value*] | **length** [*queue-length*] } **radio** [*radio-id*]
Parameter Description	**back-ground**: Sets the back-ground queue. **best-effort**: Sets the best-effort queue. **video**: Sets the video queue. **voice**: Sets the voice queue. *aifsn-value*: Sets the aifsn value, in the range from 1 to 15. *cwmin-value*: Sets the cwmin value, in the range from 0 to 15. *cwmax-value*: Sets the cwmax value, in the range from 0 to 15. *txop-value*: Sets the txop value, in the range from 0 to 255 in the unit of 32 microseconds.

	queue-length: Sets the AC queue length, in the range from 1 to 768. The default is 768. *radio-id*: Sets the EDCA parameters on the client, in the range from 1 to 16.
Command Mode	AP configuration mode
Defaults	

AC	AIFS	CWmin	CWmax	TXOP
back-ground	7	4	10	0
best-effort	3	4	10	0
video	2	3	4	94
voice	2	2	3	47

Usage Guide	The parameter configuration takes effect only when the wmm service is enabled. The cwmax value must be greater than the cwmin value. Otherwise, a message indicating configuration failure is displayed.

Configuring the EDCA Parameters on the AP Side

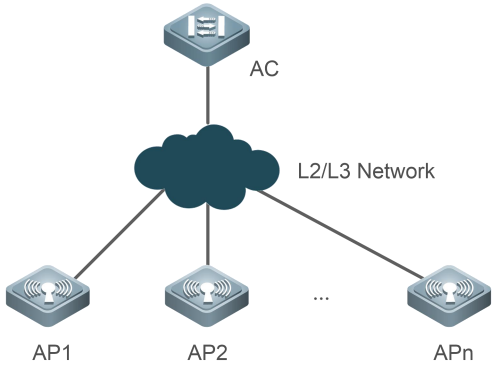
Command	**wmm edca-radio** { **back-ground** | **best-effort** | **video** | **voice** } { **aifsn** [*aifsn-value*] **cwmin** [*cwmin-value*] **cwmax** [*cwmax-value*] **txop** [*txop-value*] | **noack** } **radio** [*radio-id*]
Parameter Description	**back-ground**: Sets the back-ground queue. **best-effort**: Sets the best-effort queue. **video**: Sets the video queue. **voice**: Sets the voice queue. *aifsn-value*: Sets the aifsn value, in the range from 1 to 15. *cwmin-value*: Sets the cwmin value, in the range from 0 to 15. *cwmax-value*: Indicates setting of the cwmax value, in the range from 0 to 15. *txop-value*: Sets the txop value, in the range from 0 to 255 in the unit of 32 microseconds. **noack**: Enables the no ack policy. The no ack policy is not enabled by default. *radio-id*: Sets radio of the EDCA parameters on the client, in the range from 1 to 2.
Command Mode	AP configuration mode
Defaults	

AC	AIFS	CWmin	CWmax	TXOP
back-ground	7	4	10	0
best-effort	3	4	6	0
video	1	3	4	94
voice	1	2	3	47

Usage Guide	The parameter configuration takes effect only when the wmm service is enabled. The cwmax value must be greater than the cwmin value. Otherwise, a message indicating configuration failure is displayed.

Configuration Examples

Configuring EDCA Parameters

Scenario **Figure 1-8**	
Configuration Steps	● Configure the EDCA parameters on the client of AP1 Radio1 on the AC. ● Configure the EDCA parameters on the AP of AP1 Radio1 on the AC.
AC	FS#configure terminal FS(config)#ap-config AP1 FS(config-ap)#wmm edca-client voice aifsn 2 cwmin 2 cwmax 3 txop 50 radio 1 FS(config-ap)#wmm edca-radio voice aifsn 1 cwmin 1 cwmax 3 txop 50 radio 1
Verification	After configuring the EDCA parameters, you can display the configuration information of the EDCA parameters for a check. ● You can run the **show ap-config running** command to display the configuration information of the EDCA parameters.
	FS#show ap-config running AP1 ! ap-config AP1 wmm edca-client voice aifsn 2 cwmin 2 cwmax 3 txop 50 radio 1 wmm edca-radio voice aifsn 1 cwmin 1 cwmax 3 txop 50 radio 1 no 11acsupport enable radio 1 no 11acsupport enable radio 2 802.11n mcs support 15 radio 1 802.11n mcs support 15 radio 2 antenna receive 3 radio 1 antenna receive 3 radio 2 antenna transmit 3 radio 1 antenna transmit 3 radio 2 radio-type 1 802.11b radio-type 2 802.11a beacon period 300 radio 1 beacon period 100 radio 2 ap-mac 001a.a9c5.3f49 no enable-radio 1

	no enable-radio 2 !

Common Errors

None.

1.4.7 Configuring the Allowed Access Signal Strength

Configuration Effect

- You can control the Beacon frame broadcast coverage of the AP to prevent access of remote wireless users. You can also limit the minimum value of the RSSI for wireless users. When the RSSI of the request frame sent from a wireless user is smaller than this minimum value, the access of this wireless user is prohibited.

Notes

- If the minimum RSSI for wireless user access is set to too great, many wireless users may fail to access the WLAN.
- If the management frame transmit power is set to too great, many remote wireless users may fail to discover the network.

Configuration Steps

Configuring the Minimum RSSI for Wireless User Access

- Optional configuration. By default, the minimum RSSI for wireless user access is 0. That is, all users are allowed to access the WLAN, no matter how large the RSSI is.
- Unless otherwise specified, the configuration shall be performed in AP configuration mode on the AC device.

Configuring the Management Frame Transmit Power

- Optional configuration. By default, the management frame transmit power is 0. That is, the management frame transmit power is not configured by default.
- Unless otherwise specified, the configuration shall be performed in AP configuration mode on the AC.

Verification

- You can run the **show ap-config running** command to display the configuration information of the allowed access signal strength.

Related Commands

Configuring the Minimum RSSI for Wireless User Access

Command	**response-rssi** *rssi* **radio** *radio-id*
Parameter Description	*rssi*: Specifies the minimum RSSI for wireless user access, in the range from 0 to 100 in the unit of dB. *radio-id*: Specifies the ID of the radio to be configured, in the range from 1 to 16.
Command Mode	AP configuration mode

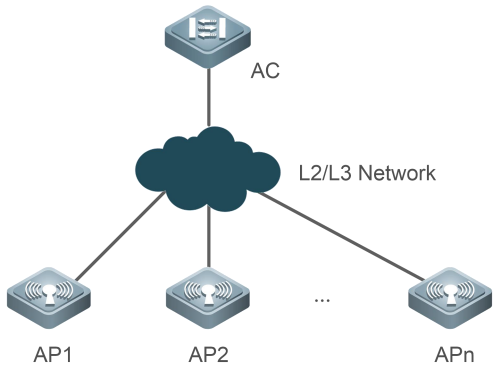
Defaults	The default RSSI is 0.
Usage Guide	N/A

Configuring the Management Frame Transmit Power

Command	**coverage-area-control** *power* **radio** *radio-id*
Parameter Description	*power*: Specifies the management frame transmit power, in the range from 0 to32 in the unit of dBm. *radio-id*: Specifies the ID of the radio to be configured, in the range from 1 to 48.
Command Mode	AP configuration mode
Defaults	The default power is 0.
Usage Guide	N/A

Configuration Examples

Configuring the Allowed Access Signal Strength

Scenario **Figure 1-9**	
Verification	● Set the minimum RSSI for wireless user access of AP1 Radio1 to 20 dB on the AC. ● Set the management frame transmit power of AP1 Radio1 to 30 dBm on the AC.
AC	FS#configure terminal FS(config)#ap-config AP1 FS(config-ap)#response-rssi 20 radio 1 FS(config-ap)#coverage-area-control 30
Configuration Steps	After configuring the allowed access signal strength, you can display the configuration information of the allowed access signal strength for a check. ● You can run the **show ap-config running** command to display the configuration information of the allowed access signal strength.
	FS#show ap-config running AP1

```
!
ap-config AP1
 ap-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024
 no 11acsupport enable radio 1
 no 11acsupport enable radio 2
 802.11n mcs support 15 radio 1
 802.11n mcs support 15 radio 2
 rts-threshold 800 radio 1
 coverage-area-control 30
 response-rssi 20 radio 1
 antenna receive 3 radio 1
 antenna receive 3 radio 2
 antenna transmit 3 radio 1
 antenna transmit 3 radio 2
 radio-type 1 802.11b
 radio-type 2 802.11a
 beacon period 300 radio 1
 beacon period 100 radio 2
 ap-mac 001a.a9c5.3f49
 no enable-radio 1
 no enable-radio 2
!
```

Common Errors

None.

1.4.8 Configuring the Number of Access Users Allowed by the AP

Configuration Effect

- Limit the STA number for the AP to implement load balancing to a certain extent, avoiding uneven distribution of AP access users.

Notes

- None.

Configuration Steps

Configuring AP-Based STA Number Limit

- Optional configuration. By default, the AP-based STA number limit is 32.
- Unless otherwise specified, the configuration shall be performed in AP configuration mode on the AC device.

Verification

- You can run the **show ap-config running** command to display the configuration information of the AP-based STA number limit.

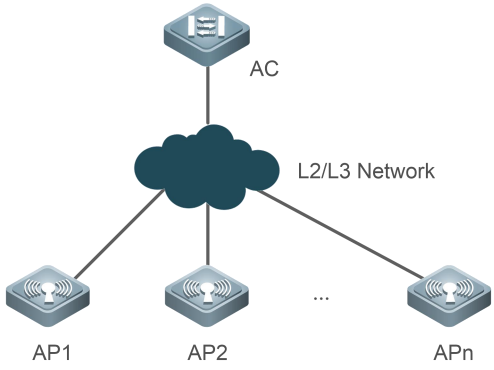
Related Commands

Configuring AP-Based STA Number Limit

Command	**sta-limit** *max-num*
Parameter Description	*max-num*: Specifies the AP-based STA number limit, in the range from 1 to 32.
Command Mode	AP configuration mode
Defaults	The default limit is 32.
Usage Guide	N/A

Configuration Examples

Configuring AP-Based STA Number Limit

Scenario **Figure 1- 10**	
Configuration Steps	● Set the number of access users allowed by AP1 to 12 on the AC.
AC	FS#configure terminal FS(config)#ap-config AP1 FS(config-ap)#sta-limit 12
Verification	After configuring the number of access users allowed by the AP, you can display the configuration information of the number of access users allowed by the AP for a check. ● You can run the **show ap-config running** command to display the configuration information of the number of access users allowed by the AP.
	FS#show ap-config running AP1 ! ap-config AP1 ap-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024 no 11acsupport enable radio 1 no 11acsupport enable radio 2 802.11n mcs support 15 radio 1

	802.11n mcs support 15 radio 2 rts-threshold 800 radio 1 coverage-area-control 30 response-rssi 20 radio 1 antenna receive 3 radio 1 antenna receive 3 radio 2 antenna transmit 3 radio 1 antenna transmit 3 radio 2 radio-type 1 802.11b radio-type 2 802.11a sta-limit 12 beacon period 300 radio 1 beacon period 100 radio 2 ap-mac 001a.a9c5.3f49 no enable-radio 1 no enable-radio 2 !

Common Errors

None.

1.4.9 Configuring a Pure 11n Network

Configuration Effect

- Configure a pure 11n network to prohibit access of non-11n devices; make all the 11n devices of the network to use pure HT header for transmission; reduce the size of the packet header; increase the available channel bandwidth for the wireless users.

Notes

- Pure 11n network does not allow access of non-11n devices.

Configuration Steps

Configuring Whether to Support 11a or Not

- Optional configuration. By default, access of 11a users at 5 GHz is supported.
- This configuration takes effect only when the radio of the AP operates at 5 GHz.

Configuring Whether to Support 11b or Not

- Optional configuration. By default, access of 11b users at 2.4 GHz is supported.
- This configuration takes effect only when the radio of the AP operates at 2.4 GHz.

Configuring Whether to Support 11g or Not

- Optional configuration. By default, access of 11g users at 2.4 GHz is supported.
- This configuration takes effect only when the radio of the AP operates at 2.4 GHz.

Configuring Whether to Support 11na or Not

- Optional configuration. By default, access of 11n users at 5 GHz is supported.
- This configuration takes effect only when the radio of the AP operates at 5 GHz.

Configuring Whether to Support 11ng or Not

- Optional configuration. By default, access of 11n users at 2.4 GHz is supported.
- This configuration takes effect only when the radio of the AP operates at 2.4 GHz.

Verification

- You can run the **show ap-config running** command to display the configuration information of the pure 11n network.

Related Commands

Configuring Whether to Support 11a or Not

Command	**11asupport enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of the radio to be configured, in the range from 1 to 16.
Command Mode	AP configuration mode
Defaults	802.11a is supported by default.
Usage Guide	This configuration takes effect only when the radio of the AP operates at 5 GHz. Configuration for all APs is not supported.

Configuring Whether to Support 11b or Not

Command	**11bsupport enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of the radio to be configured, in the range from 1 to 16.
Command Mode	AP configuration mode
Defaults	802.11b is supported by default.
Usage Guide	This configuration takes effect only when the radio of the AP operates at 2.4 GHz. Configuration for all APs is not supported.

Configuring Whether to Support 11g or Not

Command	**11gsupport enable radio** *radio-id*

Parameter Description	*radio-id*: Specifies the ID of the radio to be configured, in the range from 1 to 16.
Command Mode	AP configuration mode
Defaults	802.11g is supported by default.
Usage Guide	This configuration takes effect only when the radio of the AP operates at 2.4 GHz. Configuration for all APs is not supported.

Configuring Whether to Support 11na or Not

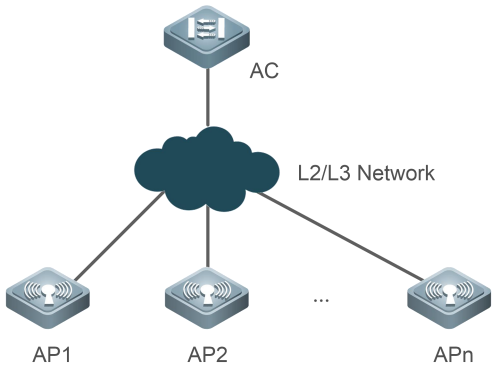
Command	**11nasupport enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of the radio to be configured, in the range from 1 to 16.
Command Mode	AP configuration mode
Defaults	802.11n at 5GHz is supported by default.
Usage Guide	This configuration takes effect only when the radio of the AP operates at 5 GHz. Configuration for all APs is not supported.

Configuring Whether to Support 11ng or Not

Command	**11ngsupport enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of the radio to be configured, in the range from 1 to 16.
Command Mode	AP configuration mode
Defaults	802.11n at 2.4GHz is supported by default.
Usage Guide	This configuration takes effect only when the radio of the AP operates at 2.4 GHz. Configuration for all APs is not supported.

Configuration Examples

Configuring a Pure 11n Network

Scenario **Figure 1-11**	 ● AP1 Radio1 operates at 2.4 GHz. ● AP1 Radio2 operates at 5.8 GHz.
Configuration Steps	● Configure AP1 Radio1 as a pure 11n network on the AC device. ● Configure AP1 Radio2 as a pure 11n network on the AC device.
AC	FS#configure terminal FS(config)#ap-config AP1 FS(config-ap)#no 11bsupport enable radio 1 FS(config-ap)#no 11gsupport enable radio 1 FS(config-ap)#11ngsupport enable radio 1 FS(config-ap)#no 11asupport enable radio 2 FS(config-ap)#11nasupport enable radio 2
Verification	After configuring a pure 11n network, you can display the configuration information of the pure 11n network for a check. ● You can run the **show ap-config running** command to display the configuration information of the pure 11n network.
	FS#show ap-config running AP1 ! ap-config AP1 ap-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024 no 11asupport enable radio 2 no 11bsupport enable radio 1 no 11gsupport enable radio 1 no 11acsupport enable radio 1 no 11acsupport enable radio 2 802.11n mcs support 15 radio 1 802.11n mcs support 15 radio 2 rts-threshold 800 radio 1 coverage-area-control 30 response-rssi 20 radio 1 antenna receive 3 radio 1 antenna receive 3 radio 2

	antenna transmit 3 radio 1 antenna transmit 3 radio 2 radio-type 1 802.11b radio-type 2 802.11a sta-limit 12 beacon period 300 radio 1 beacon period 100 radio 2 ap-mac 001a.a9c5.3f49 no enable-radio 1 no enable-radio 2 !

1.4.10 Configuring Spectrum Navigation

Configuration Effect

- The spectrum navigation function of the WLAN is enabled, guiding access of the dual-band STA to the 5G frequency band.

Configuration Steps

Enabling the Spectrum Navigation Function of the WLAN

- Mandatory configuration.
- Unless otherwise specified, this configuration shall be performed on the AC or fat AP.

Configuring the Lower Limit of STA Signal Strength Accepted by Spectrum Navigation

- Optional configuration. This configuration is performed when the spectrum navigation coverage needs to be adjusted.
- Unless otherwise specified, this configuration shall be performed on the AC or fat AP.

Configuring the Number of Times for Which Dual-Band STA Access to 2.4G Band is Denied

- Optional configuration. This configuration is performed when dual-band STA access to 2.4G band needs to be denied. If access of many dual-band STAs lasts for a very long time or fails after the configuration, you need to set a lower value or remove the configuration.
- Unless otherwise specified, this configuration shall be performed on the AC or fat AP.

Configuring the STA Information Aging Time

- Optional configuration. If no dual-band STA switches to a single-band 2.4G STA in the environment, you can configure a relatively large aging time. Otherwise, you can configure a relatively small aging time. If you cannot determine whether this type of switching occurs in the environment, use the default configuration.
- Unless otherwise specified, this configuration shall be performed on the AC or fat AP.

Configuring the Detection Period Count of Suppression STA

- Optional configuration. If a single-band 2.4G STA cannot discover the WLAN for a long time, you shall decrease the value.
- Unless otherwise specified, this configuration shall be performed on the AC or fat AP.

Configuring the Threshold of STA Detection Scanning Period

- Optional configuration. If a single-band 2.4G STA cannot discover the WLAN for a long time, you shall decrease the value. It is recommended to use the default setting if the condition is unclear.
- Unless otherwise specified, this configuration shall be performed on the AC or fat AP.

Verification

- Run the **show band-select configuration** command to display the spectrum navigation parameter configuration on the device.
- Run the **show running-config** command to display whether the spectrum navigation function is enabled for the WLAN.
- After the device operates for a certain time, run the **show band-select statistics** command to display the running statistics on the device.
- Capture packets to check whether spectrum navigation has controlled the active detection process.

Related Commands

Enabling the Spectrum Navigation Function of the WLAN

Command	**band-select enable**
Parameter Description	N/A
Command Mode	WLAN configuration mode
Defaults	Spectrum navigation is disabled by default.
Usage Guide	N/A

Configuring the Lower Limit of STA Signal Strength Accepted by Spectrum Navigation

Command	**band-select acceptable-rssi** *value*
Parameter Description	*value*: Lower limit of STA RSSI accepted by spectrum navigation, in the range from -100 to -50 in the unit of dBm.
Command Mode	Global configuration mode
Defaults	The lower limit of STA RSSI accepted by spectrum navigation is -80 dBm.
Usage Guide	N/A

Configuring the Number of Times for Which Dual-Band STA Access to 2.4G Band is Denied

Command	**band-select access-denial** *value*

Parameter Description	*value*: Number of times for which dual-band STA access to 2.4G band is denied, in the range from 0 to 10.
Command Mode	Global configuration mode
Defaults	0
Usage Guide	N/A

Configuring the STA Information Aging Time

Command	**band-select age-out** { **dual-band** *value* | **suppression** *value* }
Parameter Description	**dual-band** *value*: Aging time of dual-band STA information, in the range from 20 to 120 in the unit of seconds. **suppression** *value*: Aging time of dual-band STA information, in the range from 10 to 60 in the unit of seconds.
Command Mode	Global configuration mode
Defaults	**dual-band** *value:* 60 seconds **suppression** *value:* 20 seconds
Usage Guide	It is recommended that the aging time of dual-band STA information be set to twice to three times as much as the aging time of suppression STA information.

Configuring the Detection Period Count Value of Suppression STA

Command	**band-select probe-count** *value*
Parameter Description	*value*: Detection period count of suppression STA, in the range from 1 to 10.
Command Mode	Global configuration mode
Defaults	2
Usage Guide	N/A

Configuring the Threshold of STA Detection Scanning Period

Command	**band-select scan-cycle** *value*
Parameter Description	*value*: Threshold of STA detection scanning period, in the range from 1 to 1000 in the unit of milliseconds.
Command	Global configuration mode

Mode	
Defaults	200
Usage Guide	N/A

Displaying Spectrum Navigation-Related Configuration

Command	**show band-select configuration**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Display spectrum navigation-related configuration, including acceptable lower limit of STA signal strength, number of times for which dual-band STA access to 2.4G band is denied, aging time of STA information, detection period count of suppression STA, and threshold of STA detection scanning period.

Displaying Running Statistics of Spectrum Navigation

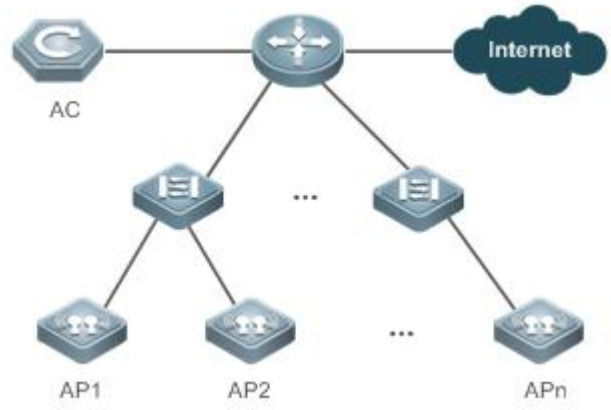
Command	**show band-select statistics**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Display running statistics of spectrum navigation, including the number of current dual-band STAs, number of identified dual-band STAs, quantity of aged dual-band STAs, quantity of current suppression STAs, number of identified suppression STAs, and number of aged suppression STAs.

Displaying Device Running Configuration

Command	**show running-config**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Display device running configuration information. The command output mainly includes spectrum navigation configuration items of WLAN configuration.

Configuration Examples

Configuring WLAN Spectrum Navigation for Fit AP Architecture

Scenario Figure 1-12	 The preceding figure shows a wireless network of typical fit AP architecture. ● AC represents a wireless access controller. ● AP1, AP2… and AP*n* are all dual-band APs. ● The AC and APs are connected by layer 2 switching device and layer 3 routing device. ● To configure spectrum navigation WLAN as WLAN 99 with SSID "wlan-bandselect", map the WLAN to the two RF interfaces to all dual-band APs.
Configuration Steps	● Configure spectrum navigation parameters on the AC (optional). ● Enable the spectrum navigation function of WLAN 99 on the AC.
AC	AC# configure terminal AC(config)# wlan-config 99 AC(config-wlan)# band-select enable
Verification	Use a dual-band STA to access WLAN "wlan-bandselect". ● Make the STA access the 5G frequency band. (The navigation may fail, and the STA may access the 2.4G frequency band.) ● Display the running statistics of spectrum navigation on the AC, and verify that the count increases.
AC	A# show band-select statistics Band Select Statistics Number of dual band client..... 1 Number of dual band client added..... 1 Number of dual band client expired..... 0 Number of suppressed client..... 0 Number of suppressed client added..... 0 Number of suppressed client expired..... 0

Common Errors

- Spectrum navigation parameters are improperly configured.

- The spectrum navigation function is not enabled.
- One of the two RF interfaces of the dual-band AP is disabled.

1.4.11 Configuring One-Click Network Optimization

Configuration Effect

- Improve the network performance.

Configuration Steps

Configuring Network Optimization Options

- Optional.
- Enable network optimization on the AC unless otherwise specified.
- Run the **wopt choose** command to configure network optimization options. At least one option is selected.
- Network optimization options can be configured via the network optimization function to improve network performance. Users can select network optimization options based on recommended configurations and actual network conditions. The **no** form is not supported to restore the configurations before optimization. Therefore, if the configurations are incorrect, modify the configurations in corresponding mode.

Command	**wopt choose** { **band-select-disable** | **band-select-enable** | **low-rate-disable** | **multicast-speed** | **rrm-disable** | **rrm-enable** | **session-limit** | **speed-limit** }
Parameter Description	**band-select-disable**: Disables the 5 GHz preferred function. If only few STAs supporting 5 GHz exist in the environment, it is recommended that the 5 GHz preferred function be disabled. **band-select-enable**: Enables the 5 GHz preferred function. If a large number of STAs supporting 5 GHz exist in the environment, it is recommended that the 5 GHz preferred function be enabled. **low-rate-disable**: Forbids low-rate packets. Packets with a rate lower than 11 Mbps are forbidden. **multicast-speed**: Restores the default multicast rate (24 Mbps). **rrm-disable**: Disables the RRM function. If no intra-frequency or inter-frequency interference exists in the environment, it is recommended that the RRM function be disabled. **rrm-enable**: Enables the RRM function. If intra-frequency or inter-frequency interference exists in the environment, it is recommended that the RRM function be enabled to perform channel or power adjustment. **session-limit**: Restores the default number of sessions. The number of sessions affects authentication page pushing by iPortal. It is recommended that the default number of sessions be used. The default number of sessions is 255 for each STA and 1000 for each port. **speed-limit**: Limits the rate. (Rate limiting is performed for all STAs by WLAN. The average uplink and downlink rate is 256 kbit/s and the abrupt rate is 300 kbit/s.)
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	Select network optimization options based on environment requirements. Restoring to the configurations before network optimization is not supported. Therefore, exercise caution when selecting network optimization options. If incorrect configurations are optimized, modify the configurations in corresponding configuration mode manually.

Configuring One-Click Network Optimization

- Optional.
- Enable network optimization on the AC unless otherwise specified.
- Run the **wopt enable** command to configure one-click network optimization.
- One-click network optimization can be configured via the network optimization function to improve network performance. The **no** form is not supported to restore the configurations before optimization. Therefore, if the configurations are incorrect, modify the configurations in corresponding mode.

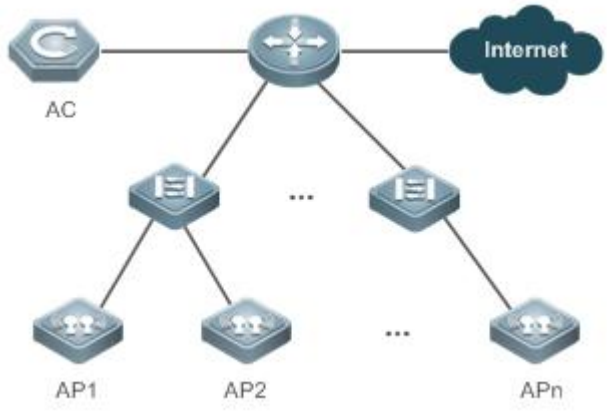
Command	**wopt enable**
Parameter Description	N/A
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	One-click network optimization can be configured if it is required to forbid low-rate packets, restore default multicast rates for WLANs, restore the default number of sessions, and limit rates for WLANs (average uplink and downlink rate is 256 kbit/s and abrupt rate is 300 kbit/s) in an actual environment. Note: Restoring to the configurations before network optimization is not supported. Therefore, exercise caution when configuring one-click network optimization. If incorrect configurations are optimized, modify the configurations in corresponding configuration mode manually.

Verification

- Run the **show wopt** command to display network optimization information.

Configuration Example

Configuring Network Optimization Options in a Fit AP Architecture

Scenario **Figure 1-13**	 The preceding figure shows a typical wireless network with the fit AP architecture. ● AC is the wireless network controller. ● AP1, AP2, ….APn are dual-band APs.

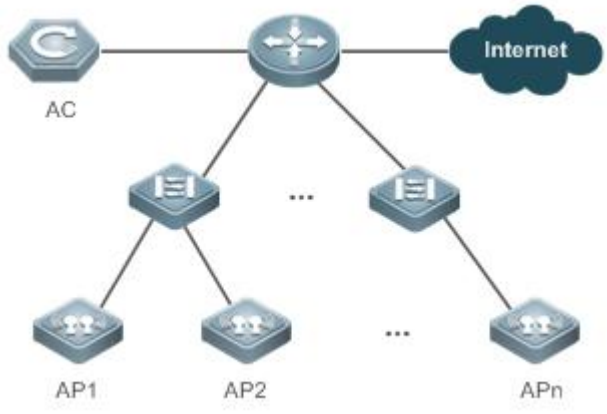
	● The AC and AP are connected through a layer-2 switch and layer-3 router. ● Many STAs supporting 5 GHz exist in the environment. Therefore, it is recommended that the 5 GHz preferred function be enabled, that is, the spectrum navigation function be enabled. ● Low-rate packets are forbidden.
Configuration Steps	● Configure network optimization options on the AC.
AC	AC# configure terminal AC(config)# wopt choose band-select-enable low-rate-disable
Verification	After the user configures network optimization options, display the network optimization information for verification. ● Run the **show wopt** command to display network optimization information.
AC	AC# show wopt Low rate status: 802.11b rate: 1 Mbps: Disable 2 Mbps: Disable 5.5 Mbps: Disable 11 Mbps: Enable 802.11g rate: 1 Mbps: Disable 2 Mbps: Disable 5.5 Mbps: Disable 6 Mbps: Disable 9 Mbps: Disable 11 Mbps: Enable 802.11a rate: 6 Mbps: Disable 9 Mbps: Disable Multicast rate: 1 24 Mbps 2 24 Mbps 3 24 Mbps 4 24 Mbps 5 24 Mbps 6 24 Mbps 7 24 Mbps 8 24 Mbps 11 24 Mbps 12 24 Mbps

```
13      24    Mbps
14      24    Mbps
15      24    Mbps
16      24    Mbps
17      24    Mbps
18      24    Mbps
19      24    Mbps
100     24    Mbps
1000 24    Mbps
1048 24    Mbps

Session limit:
  Session limit : 255

wlan 1, Band select: enable
  -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 2, Band select: enable
  -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 3, Band select: enable
  -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 4, Band select: enable
  -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 5, Band select: enable
  -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 6, Band select: enable
  -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 7, Band select: enable
  -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 8, Band select: enable
  -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 11, Band select: enable
  -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 12, Band select: enable
  -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.
```

```
wlan 13, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 14, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 15, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 16, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 17, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 18, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 19, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 100, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 1000, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 1048, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

RRM status:
RRM 11a status: dca[disable] mode[NA]
                tpc[disable] mode[NA]
RRM 11b status: dca[disable] mode[NA]
                tpc[disable] mode[NA]
 -----> If there are co-channel and adjacent channel interference, suggest to enable RRM.

Speed limit:
 wlan[1    ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
 wlan[2    ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
 wlan[3    ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
 wlan[4    ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
 wlan[5    ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
 wlan[6    ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
```

	wlan[7] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[8] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[11] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[12] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[13] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[14] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[15] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[16] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[17] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[18] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[19] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[100] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[1000] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[1048] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]

Configuring One-Click Network Optimization in Fit AP Architecture

Scenario Figure 1-14	 The preceding figure shows a typical wireless network with the fit AP architecture. ● AC is the wireless network controller. ● AP1, AP2, ….APn are dual-band APs. ● The AC and AP are connected through a layer-2 switch and layer-3 router. ● One-click network optimization is to be configured.
Configuration Steps	● Configure one-click network optimization on the AC.
AC	AC# configure terminal AC(config)# wopt choose band-select-enable low-rate-disable
Verification	After one-click network optimization is configured, display the network optimization information for verification. ● Run the **show wopt** command to display network optimization information.
AC	AC# show wopt

```
Low rate status:
  802.11b rate:
        1 Mbps: Disable
        2 Mbps: Disable
    5.5 Mbps: Disable
       11 Mbps: Enable
  802.11g rate:
        1 Mbps: Disable
        2 Mbps: Disable
    5.5 Mbps: Disable
        6 Mbps: Disable
        9 Mbps: Disable
       11 Mbps: Enable
  802.11a rate:
        6 Mbps: Disable
        9 Mbps: Disable

Multicast rate:
1       24    Mbps
2       24    Mbps
3       24    Mbps
4       24    Mbps
5       24    Mbps
6       24    Mbps
7       24    Mbps
8       24    Mbps
11      24    Mbps
12      24    Mbps
13      24    Mbps
14      24    Mbps
15      24    Mbps
16      24    Mbps
17      24    Mbps
18      24    Mbps
19      24    Mbps
100     24    Mbps
1000 24    Mbps
1048 24    Mbps

Session limit:
  Session limit : 255

wlan 1, Band select: enable
  -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.
```

```
wlan 2, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 3, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 4, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 5, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 6, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 7, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 8, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 11, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 12, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 13, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 14, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 15, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 16, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 17, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 18, Band select: enable
```

```
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 19, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 100, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 1000, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 1048, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

RRM status:
RRM 11a status: dca[disable] mode[NA]
                tpc[disable] mode[NA]
RRM 11b status: dca[disable] mode[NA]
                tpc[disable] mode[NA]
 -----> If there are co-channel and adjacent channel interference, suggest to enable RRM.

Speed limit:
 wlan[1    ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
 wlan[2    ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
 wlan[3    ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
 wlan[4    ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
 wlan[5    ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
 wlan[6    ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
 wlan[7    ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
 wlan[8    ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
 wlan[11   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
 wlan[12   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
 wlan[13   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
 wlan[14   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
 wlan[15   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
 wlan[16   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
 wlan[17   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
 wlan[18   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
 wlan[19   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
 wlan[100 ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
 wlan[1000] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
 wlan[1048] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]
```

1.4.12 Configuring Intelligent Network Optimization

Configuration Effect

- Perform intelligent network optimization based on network conditions.

Configuration Steps

- Run the **wis enable** command in configuration mode.

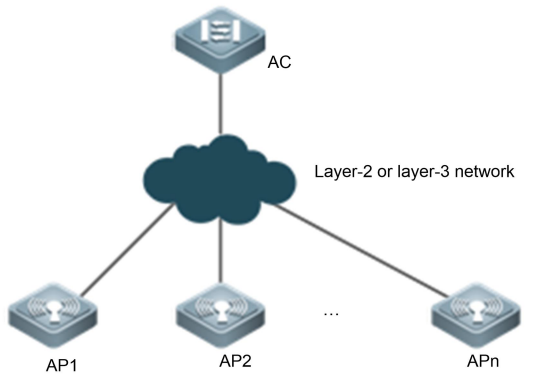
Command	**wis enable**
Parameter Description	N/A
Defaults	Intelligent network optimization is not configured by default.
Command Mode	AC global configuration mode
Usage Guide	After this command is run on a running network, intelligent optimization can be performed for the network. In normal cases, this command is used by network management personnel.

Verification

- Run the **show running** command to display the configurations.

Configuration Example

Configuring Intelligent Network Optimization

Scenario Figure 1-15	
Configuration Steps	● Enable intelligent network optimization on the AC.
AC	FS#configure terminal FS(config-ac)#wis enable
Verification	After intelligent network optimization is configured, display the configurations for verification. ● Run the **show running** command to display information about intelligent network optimization.

	FS#show running ! wis enable !

1.4.13 Configuring Mcell

Configuration Effect

- Enable dense deployment optimization.

Configuration Steps

- Run the **mcell** command in AP configuration mode.

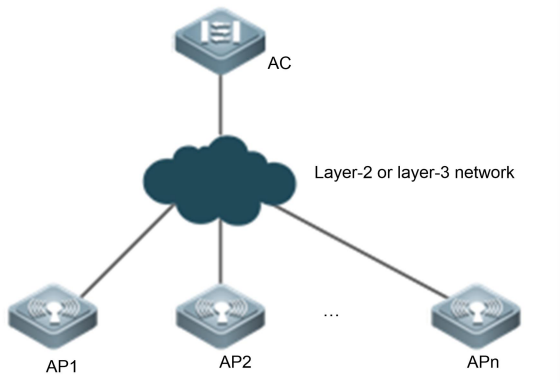
Command	mcell enable **radio** *radio-id*
Parameter Description	*radio-id*: Indicates the index of an RF port. The value range is 1 to 16.
Defaults	Mcell is disabled by default.
Command Mode	AP configuration mode
Usage Guide	N/A

Verification

- Run the **show running** command to display the configurations.

Configuration Example

Configuring Mcell

Scenario **Figure 1-16**	
Configuration Steps	- Enable the Mcell function on the AC.

AC	FS#configure terminal FS(config)#ap-config AP1 FS(config-ap)# mcell enable radio 1
Verification	After the Mcell function is configured, display the configurations for verification. ● Run the **show running** command to display information about the Mcell function.
	FS#show ap-config running ap-config AP1 mcell enable radio 1

1.4.14 Configuring Roaming Stickiness

Configuration Effect

- Configure this function to enable roaming stickiness monitoring or navigation.

Notes

- The WIS must be enabled.

Configuration Steps

- Configure roaming stickiness in ap-config all or ap-group configuration mode.

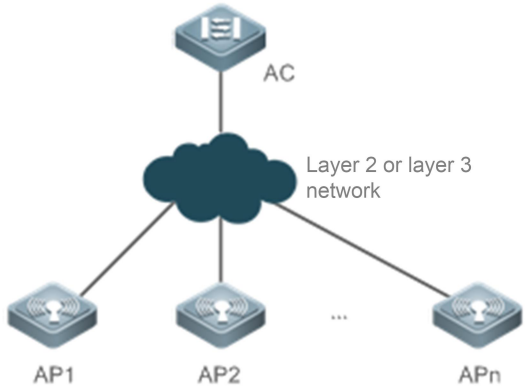
Command	**sticky-steering** { **monitor-only** | **enable** }
Parameter Description	**monitor-only**: Indicates the monitoring mode, that is, only roaming stickiness is monitored. **enable**: Indicates the navigation mode, that is, roaming stickiness navigation is performed if roaming stickiness is detected.
Defaults	By default, roaming stickiness is disabled.
Command Mode	Configure roaming stickiness for all AP groups in ap-config all mode, and configure roaming stickiness for a single AP group in ap-group mode.
Usage Guide	N/A

Verification

- Run **show running** to query the corresponding configuration.

Configuration Example

Configuring Roaming Stickiness

Scenario **Figure 1-17**	
Configuration Steps	● Configure roaming stickiness monitoring on the AC. ● Configure roaming stickiness navigation on the AC.
AC	FS#configure terminal FS(config)#ap-config all FS(config-ap)# sticky-steering monitor-only FS(config-ap)# ap-group test1 FS(config-group)#sticky-steering enable
Verification	● Run **show running** to query the roaming stickiness configuration information.

	FS#show running-config
	ap-group test1
	  sticky-steering enable
	!
	ap-group test2
	  sticky-steering monitor-only
	!
	ap-group test3
	  sticky-steering monitor-only
	!

1.4.15 Configuring Remote Association Information Collection

Configuration Effect

- Enable remote association information collection to enable the WIS client to provide remote association optimization solutions.

Notes

- The WIS must be enabled.

Configuration Steps

- Enable remote association information collection in ap-config all or ap-group configuration mode.

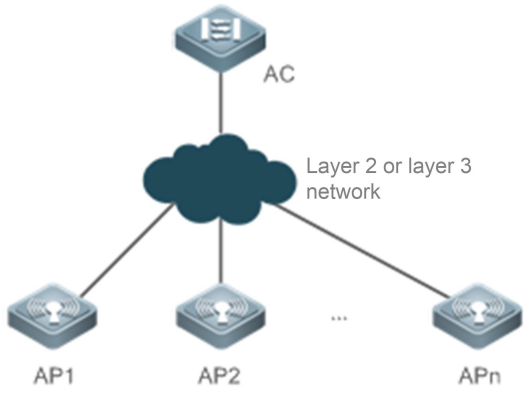
Command	**farpoint-steering enable**
Parameter Description	**enable**: Indicates that remote association information collection is enabled.
Defaults	By default, the remote association information collection function is disabled.
Command Mode	Enable remote association information collection for all AP groups in ap-config all mode and for a single AP group in ap-group mode.
Usage Guide	N/A

Verification

- Run **show running** to query the corresponding configuration.

Configuration Example

Configuring Remote Association Information Collection

Scenario Figure 1- 18	
Configuration Steps	● Enable remote association information collection on the AC.
AC	FS#configure terminal FS(config)#ap-config all FS(config-ap)# farpoint-steering enable FS(config-ap)# ap-group test1 FS(config-group)#no farpoint-steering enable
Verification	● Run **show running** to query the configuration information about remote association information collection.
	FS#show running-config ap-group test1 ! ap-group test2 farpoint-steering enable ! ap-group test3

	farpoint-steering enable !

1.4.16 Configuring Automatic Device Information Upload

Configuration Effect

- Enable automatic upload of AC and AP software and hardware version information to the WIS cloud.

Notes

- If the WIS function is not enabled, AC and AP software and hardware version information will also be automatically uploaded after this function is enabled. The information upload priority is as follows:
- If the WIS client address is configured, the information is uploaded to the WIS client.
- If the WIS client is not configured but the device can access to the WIS public cloud, the information will be uploaded to the WIS public cloud.
- If the WIS client is not configured and the device cannot access to the WIS public cloud, the device information is not uploaded.

Configuration Steps

- Perform this operation in global configuration mode.

Command	**wis devinfo enable**
Parameter Description	**enable**: Indicates that device information is automatically uploaded.
Defaults	By default, automatic device information upload is enabled.
Command Mode	Global configuration mode
Usage Guide	N/A

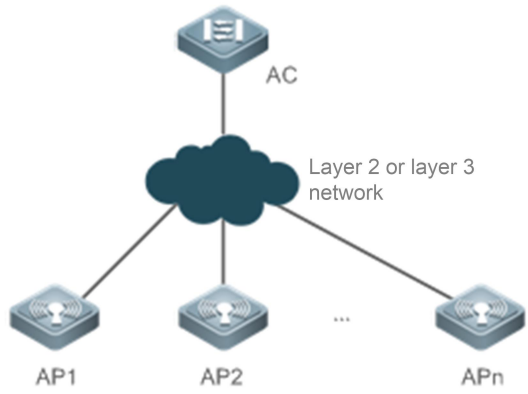
Verification

- Run **show running** to query the corresponding configuration.

Configuration Example

- N/A

Configuring Automatic Device Information Upload

Scenario **Figure 1- 19**	
Configuration Steps	● Disable automatic device information upload on the AC.
AC	FS#configure terminal FS(config)# no wis devinfo enable
Verification	● Run **show running** to query the configuration information about automatic device information upload.
	FS#show running-config no wis devinfo enable! !

1.5 Monitoring

Displaying

Function	Command
Display all configuration information.	**show running**
Display the configuration information of a specified AP.	**show ap-config running** *ap-name*
Display the radio information of all APs.	**show ap-config radio**
Display the configuration information of a specified AP's specified radio.	**show ap-config radio** *radio-id* **config** *ap-name*
Display the detailed status information of an AP's specified radio.	**show ap-config radio** *radio-id* **status** *ap-name*
Display the radio list of an AP.	**show ap-config radio status** *ap-name*
Display the running statistics of band selection.	**show band-select statistics**
Display the network optimization information.	**show wopt**

2 Configuring Band Select

2.1 Overview

Band Select is a technology for optimizing access band distribution for STAs on a WLAN.

The Band Select function leads dual-band STAs to access the higher-capacity 5 GHz band to reduce the pressure on the 2.4 GHz band and improve user experience.

The Band Select function is suitable for the following scenario: dual-band APs are used to provide coverage, and the two RF interfaces of the APs operate at 2.4 GHz and 5 GHz respectively; meanwhile, a WLAN is mapped to the two RF interfaces of the APs and provides access service at the two bands simultaneously.

Protocols and Standards

- IEEE 802.11

2.2 Applications

Application	Description
Band Select for a WLAN Using a Fit AP Architecture	In a fit AP architecture, a WLAN composed of multiple dual-band APs is enabled with the Band Select function.

2.2.1 Band Select for a WLAN Using a Fit AP Architecture

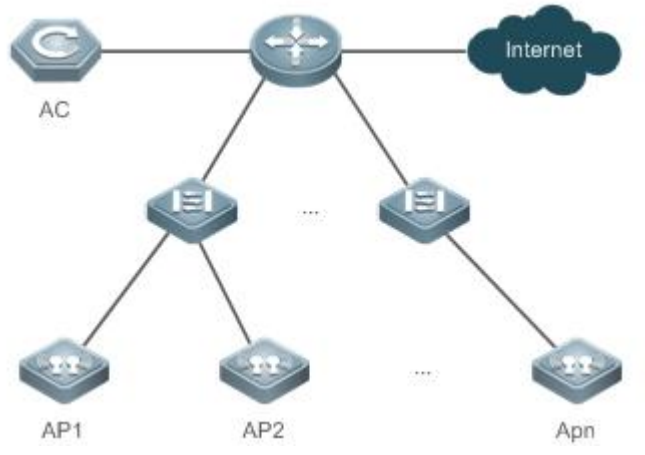
Scenario

In a fit AP architecture, a WLAN composed of multiple dual-band APs is enabled with the Band Select function,

as shown in Figure 2-1,

- One AC is associated with multiple dual-band APs. The AC and APs are connected through layer-2 switch devices and layer-3 routers.
- The WLAN is mapped to the two RF interfaces of all dual-band APs.

Figure 2-1



Remarks	AC is a wireless access controller. AP_1, AP_2 … AP_n are dual-band APs.

Deployment

- Manage parameters of the Band Select function on the AC.
- Apply the Band Select function, identifies STA types and leads STA access on the AC.

2.3 Features

Basic Concepts

IEEE802.11 Communication Band

IEEE802.11 comprises two communication bands:

- 2.4 GHz (2.4 to 2.4835 GHz), where 802.11b/g/n resides
- 5 GHz (5.15 to 5.35 and 5.725 to 5.825 GHz), where 802.11a/n resides

With the popularization of WLANs, there are more and more wireless users. Many users use dual-band wireless clients (STAs) supporting both 2.4 GHz and 5 GHz. However, 802.11b/g is more widely applied than 802.11a. Many dual-band STAs use 2.4 GHz, causing congestion of 2.4 GHz and waste of 5 GHz. Actually, the 5 GHz band has a greater access capacity. The 2.4 GHz band has up to three non-overlapped channels, whereas the 5 GHz band provides more non-overlapped channels.

STA Scanning

There are two modes, namely, passive scanning and active scanning.

- Passive scanning: An STA monitors beacon frames sent by nearby APs on all channels of all supported bands. The beacon frames contain WLAN access information. The STA parses the information to learn about the WLANs that are available nearby.
- Active scanning: The STA broadcasts a Probe Request frame on all channels of all supported bands. After receiving the Probe Request frame, the APs providing WLAN access service sends a Probe Response frame including some WLAN information to the STA.

Generally, the STA summarizes the SSIDs of all discovered WLANs and provides an accessible WLAN list for users.

Dual-band STA

WLAN network interface cards (WNICs) used by STAs to connect to WLANs are classified into a, b, g and n types, which indicate the 802.11 protocol types supported by the WNICs. 802.11a operates at 5 GHz, 802.11b/g at 2.4 GHz, and 802.11n at 5 GHz and 2.4 GHz.

Therefore, if the specification of a WNIC includes both a and b/g, this WNIC supports both the two bands, namely, a dual-band STA. A dual-band STA can access both the 5 GHz band and the 2.4 GHz band.

Dual-band AP

A dual-band AP is able to access two bands. Therefore, a dual-band AP requires at least two RF interfaces, one for 5 GHz and the other for 2.4 GHz.

A WLAN enabled with Band Select must be mapped to the two RF interfaces of the dual-band AP and provides access service at the two bands.

Overview

Feature	Description
Identifying STA Types	The Band Select function identifies whether an STA is a dual-band STA.
Controlling the Active Scanning Process	The Band Select function controls active scanning of the dual-band STA to prevent the STA from discovering WLANs of the 2.4 GHz band.
Rejecting Accessing the 2.4 GHz Band	The Band Select function rejects the dual-band STA from accessing the 2.4 GHz band and improves the chance of accessing the 5 GHz band.

2.3.1 Identifying STA Types

To lead a dual-band STA to access the 5 GHz band, you should first identify whether the STA is a dual-band STA; that is, identify the band supported by the STA.

Working Principle

Active scanning is an approach for an STA to discover WLANs. When using active scanning, the STA sends a Probe Request frame on each supported channel. If the channel information in the Probe Request frame sent by the STA can be obtained, the bands supported by the STA can be identified.

For example, if an AP receives the Probe Request frame on channels 1-13, the AP learns that the STA supports the 2.4 GHz band. If the AP receives the Probe Request frame on channels 149-165, the AP learns that the STA supports the 5 GHz band.

Since a single-band AP can receive the Probe Request frame only at one band, only a dual-band AP can correctly identify the STA type. This is why the Band Select function requires a dual-band AP be used.

STA Classification Standards

A dual-band AP classifies STAs based on the following standards:

- If the AP can receive the Probe Request frame from an STA both at the 2.4 GHz band and the 5 GHz band, this STA is a dual-band STA.
- If the AP can receive the Probe Request frame from this STA only at the 5 GHz band, the AP learns that this STA is a 5 GHz STA.
- If the AP can receive the Probe Request frame from this STA only at the 2.4 GHz band, the AP learns that this AP is a 2.4 GHz STA.

The AP must wait for a period of time to verify that no Probe Request frame is received at the band; therefore, identifying a single-band STA is time-consuming but does not affect the normal use by users. Among the three types of STAs, the first two types are called the dual-band STAs in the Band Select function and the last type is called the inhibition STAs.

It takes a period of waiting time (fixed to 2 seconds) to determine whether a Probe Request frame is sent at the 5 GHz band. Due to different STA drivers, this time is not applicable to all dual-band STAs. Therefore, STA types may not be correctly identified in the beginning. As long as dual-band STAs can send Probe Request frames at the 5 GHz band later, the correct STA types can be identified.

STA Information Saving

The STA information identified by a dual-band AP must be saved to provide the basis for subsequent responding policies.

Since Probe Request frames sent by STAs are broadcast packets, an AP may receive many Probe Request frames generally. It is unnecessary to save all the frames because some distant STAs may not access the AP. Therefore, the Band Select function saves only the information of STAs that may have access. The selection criterion is the Received Signal Strength Indication (RSSI) of STAs. Only those whose RSSI exceeds a threshold can access the AP, and only then does the identified information need to be saved.

STA Information Aging

Users can configure the bands supported by some STAs; therefore, STA type may change during use.

Take an 802.11a/g/n-supported WNIC for example. The WNIC works as a dual-band STA in the beginning. However, a user disables its 802.11a mode or the support for the 5 GHz channels. Then, the WNIC changes to a single-band 2.4 GHz STA.

In this case, an aging mechanism needs to be used for the identified STA information. After a period of time, the previously identified STA information is discarded.

2.3.2 Controlling the Active Scanning Process

After identifying the bands supported by an STA, a dual-band AP can control the active scanning of the STA according to the STA information. The purpose is to prevent a dual-band STA from discovering 2.4 GHz WLANs and thus lead the dual-band STA to access the 5 GHz band.

Working Principle

During active scanning, the STA broadcasts a Probe Request frame. After receiving the Probe Request frame, an AP sends a Probe Response frame immediately to inform the STA of the accessible WLANs on this AP. During active scanning of a dual-band STA, the STA sends a Probe Request frame and waits for a Probe Response frame on the two bands. After the Band Select function is enabled, the AP controls the active scanning and adopts different response approaches according to actual situations.

Active Scanning Before the Band Select Function Identifies STA Types

If the Band Select function is enabled for a WLAN, the WLAN may have different responses to active scanning of an STA. Before STA types are identified:

- The AP does not respond to Probe Request frames from the 2.4 GHz band.
- The AP responds to Probe Request frames from the 5 GHz band.

After receiving a Probe Request frame from the 2.4 GHz band, the AP cannot determine whether the STA supports the 5 GHz band. To prevent the STA from discovering that the WLAN provides access service at the 2.4 GHz band, the AP responds after the identification process ends.

If the AP receives a Probe Request frame from the 5 GHz band, it indicates that the STA supports the 5 GHz band. In this case, the AP sends a Probe Response frame immediately to tell the STA that WLAN provides access service at the 5 GHz band.

Active Scanning After the Band Select Function Identifies STA Types

When the AP receives a Probe Request frame after identifying the STA type, the AP can find the source MAC address in the Probe Request frame stored on the AP.

- If the STA is a dual-band STA, the AP does not respond to a 2.4 GHz Probe Request; if the STA is an inhibition STA, the AP responds negatively.
- The AP responds to a 5 GHz Probe Request.

Not responding to a 2.4 GHz Probe Request sent by a dual-band STA can prevent the dual-band STA from discovering that a WLAN provides access service at the 2.4 GHz band. In this way, the dual-band STA only discovers that the WLAN provides access service at the 5 GHz band. The dual-band STA has to select the 5 GHz band for access.

The AP must responds to the 2.4 GHz Probe Request from an inhibition STA. Since an inhibition STA supports only the 2.4 GHz band, the inhibition STA cannot identify a WLAN if the AP does not respond to the 2.4 GHz Probe Request. However, the response to an inhibition STA is negative.

A 5 GHz Probe Request is sent only by a dual-band STA. Therefore, the AP must send a Probe Response t immediately to tell the WLAN to provide access service at the 5 GHz band.

Negative Response to an Inhibition STA

The Band Select function always positively responds to 5 GHz Probe Requests, does not respond to 2.4 GHz Probe Requests sent by dual-band STAs, and responds to Probe Requests from inhibition STAs negatively.

Figuratively speaking, a negative response is a discounted response. For example, when receiving multiple Probe Requests consecutively, the AP sends only one Probe Response.

The negativity depends on two parameters: STA scanning cycle threshold and the probe count of the inhibition STA.

The STA scanning cycle refers to the time for scanning all supported channels during the active scanning of an STA. This time depends on the driver of the STA and varies with STAs. The STA scanning cycle is a value configured by users, which is considered the minimum STA scanning cycle. If the scanning cycle of an STA is smaller than this value, two consecutive scanning cycles may be considered to be one by an AP. This parameter is useful when some STAs send multiple Probe Requests within one scanning cycle.

Example: Assume that an STA scans all channels every 150 milliseconds and sends two Probe Request frames consecutively on each channel. If an AP does not specify the minimum scanning cycle of the STA, the AP cannot identify whether the STA sends two frames within the same scanning cycle or sends the two frames in two consecutive scanning cycles. If the AP sets the minimum scanning cycle of the STA to 200 milliseconds, the two frames are considered to be sent within the same scanning cycle because their interval is shorter than 200 milliseconds. The probe count of the STA on the AP is 1. Since the specified minimum scanning cycle (200 milliseconds) and the actual scanning cycle (150 milliseconds) are different, the counts are also different. Assume that the STA performs scanning for three consecutive cycles, the count on the AP will be 2 because the first two cycles are considered to be one. However, this problem does not cause inconvenience to users.

The probe count of an STA reflects the negativity of the response. This parameter indicates that an AP sends one response after an inhibition STA performs active scanning for multiple cycles. For example, if the default value is 2, the WLAN on the AP sends a Probe Response frame after the STA performs scanning for two consecutive cycles.

2.3.3 Rejecting Accessing the 2.4 GHz Band

The Band Select function controls only the active scanning of an STA, but cannot prevent the STA from discovering a 2.4 GHz WLAN through passive scanning. Therefore, some dual-band STAs can still discover 2.4 GHz WLANs and attempt to access the WLANs. In this case, the Band Select function may fail.

The Band Select function can reject 2.4 GHz access requests from dual-band STAs to improve the chance for dual-band STAs accessing the 5 GHz band.

Rejecting a dual-band STA's 2.4 GHz access request helps facilitate the Band Select function; however, the Band Select function cannot be 100% successful.

Working Principle

After an STA discovers a WLAN for a user to access the WLAN, the STA sends an Authentication Request to the AP at first. Then, the AP sends an Authentication Response to permit or reject the STA's authentication request.

The Band Select function processes the Authentication Request. If the Authentication Request is sent by a dual-band STA at the 2.4 GHz band, the function can reject the Authentication Request until the dual-band STA sends an Authentication Request from the 5 GHz band. Thus, the STA is led to access the 5 GHz band.

Generally, when a dual-band STA searches for access, the STA sends one or more Authentication Requests at a band and waits for responses. If the STA does not receive responses or fails in access, the STA sends Authentication Requests at the other band and waits for responses. However, some dual-band STAs send Authentication Requests only at the 2.4 GHz. For high availability, you can use the Band Select function to set the rejecting count for a dual-band STA.

Assume that a dual-band STA sends Authentication Requests for M times before changing the band, and the rejecting count is set to N. If the dual-band STA attempts to access the 5 GHz band at first, the STA can access the 5 GHz band immediately. If the dual-band STA attempts to access the 2.4 GHz band at first, the STA can access the 5 GHz band only if N is equal to or greater than M; otherwise, the STA accesses the 2.4 GHz band. No matter which band a dual-band STA accesses, if the dual-band STA attempts to access the 2.4 GHz band at first, min (smaller one between M and N) Authentication Requests are rejected or ignored. As a result, the STA's access is delayed. The delay time depends on the driver of the STA. For example, if the STA sends Authentication Requests at the interval of 100 milliseconds and four Authentication Requests are ignored, the access of the STA will be delayed for 400 milliseconds.

When the Band Select function rejects the access request of a dual-band STA while another access control module such as load balance accepts the access request, the STA will still gain access. This is because the Band Select function plays only the "leading" role during STA access and has a low priority. When the Band Select function conflicts with other functions, the other functions shall prevail.

2.4 Configuration

Configuration	Description and Command	
Configuring Band Select	(Mandatory) It is used to enable the Band Select function for a WLAN.	
	band-select enable	Enables the Band Select function.
	(Optional) It is used to set the parameters of the Band Select function.	
	band-select acceptable-rssi	Configures the minimum RSSI for the Band Select function.
	band-select access-denial	Configures the rejecting count for a dual-band STA's 2.4 GHz access requests.
	band-select age-out	Configures the aging time of STA information.
	band-select probe-count	Configures the probe count of an inhibition STA.
	band-select scan-cycle	Configures the scanning cycle threshold of an STA.

2.4.1 Configuring Band Select

Configuration Effect

- Enable the Band Select function for a WLAN to lead dual-band STAs to access the 5 GHz band.

Notes

- N/A

Configuration Steps

Enabling the Band Select Function for a WLAN

- Mandatory.
- If there is no special requirement, enable this function on an AC or a fat AP.

Command	**band-select enable**
Parameter Description	N/A
Defaults	The Band Select function is disabled.
Command Mode	WLAN configuration mode
Usage Guide	N/A

Configuring the Minimum RSSI for the Band Select Function

- (Optional) It is configured when you want to adjust the coverage of the Band Select function.
- If there is no special requirement, enable this function on an AC or a fat AP.
- The higher the value, the smaller the coverage of the Band Select function; the lower the value, the larger the coverage of the Band Select function. However, if the value exceeds a certain limit, the STA signals that gain access may be too weak, causing the connection rate of the entire network to slow down.

Command	**band-select acceptable-rssi** *value*
Parameter Description	*value*: Specifies the minimum SSID for the Band Select function, ranging from -100 to -50 dBm.
Defaults	The default value is -80 dBm
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Rejecting Count for a Dual-Band STA's 2.4 GHz Access Requests

- (Optional) It is configured when it is necessary to reject the 2.4 GHz access request of dual-band STAs. If many STAs fail in access or it takes much time to access, configure this parameter to a smaller value or to 0.
- If there is no special requirement, enable this function on an AC or a fat AP.
- The more the rejecting count is, the more difficult the dual-band STA accesses the 2.4 GHz band, and the later the STA accesses the 2.4 GHz band. On the other hand, the less the rejecting count is, the easier the dual-band STA accesses the 2.4 GHz band, and the sooner the STA accesses the 2.4 GHz band.

Command	**band-select access-denial** *value*
Parameter Description	*value*: Specifies the rejecting count for a dual-band STA's 2.4 GHz access requests, ranging from 0 to 10.

Defaults	The default value is 2
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Aging Time of STA Information

- (Optional) If no dual-band STAs change to single-band 2.4 GHz STAs, configure a longer aging time. Otherwise, configure a shorter aging time. If it is uncertain, use the Defaults.
- If there is no special requirement, enable this function on an AC or a fat AP.
- The longer the STA information aging time, the longer the lifecycle of STA information, and the less sensitive of an AP to STA's band change. The shorter the STA information aging time, the shorter the lifecycle of STA information, and the more sensitive of an AP to STA's band change.

Command	**band-select age-out** { **dual-band** *value* | **suppression** *value* }
Parameter Description	**dual-band** *value*: Specifies the aging time of dual-band STA information, ranging from 20 to 120 seconds. **suppression** *value*: Specifies the aging time of inhibition STA information, ranging from 10 to 60 seconds.
Defaults	The aging time of dual-band STA information is 60 seconds and the aging time of inhibition STA information is 20 seconds.
Command Mode	Global configuration mode
Usage Guide	It is recommended that the aging time of dual-band STA information be set to twice or three times that of inhibition STA information.

Configuring the Probe Count of an Inhibition STA

- (Optional) If a single-band 2.4 GHz STA cannot discover a WLAN for a long time, this parameter should be set to a smaller value.
- If there is no special requirement, enable this function on an AC or a fat AP.
- The greater the probe count of an STA, the stronger inhibition the Band Select function performs on an inhibition STA, and the more difficult the inhibition STA discovers a WLAN. On the other hand, the smaller the probe count of an STA, the weaker inhibition the Band Select function performs on an inhibition STA, and the easier the inhibition STA discovers a WLAN.

Command	**band-select probe-count** *value*
Parameter Description	*value*: Specifies the probe count of an inhibition STA, ranging from 1 to 10.
Defaults	The default value is 2.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Scanning Cycle Threshold of an STA

- (Optional) If a single-band 2.4 GHz STA cannot discover a WLAN for a long time, this parameter should be set to a smaller value. If it is uncertain, use the Defaults.
- If there is no special requirement, enable this function on an AC or a fat AP.

- The greater the scanning cycle threshold of an STA, the more slowly the probe count of the STA increases, and the more difficult the STA discovers a WLAN. On the other hand, the smaller the scanning cycle threshold of the STA, the more quickly the probe count of the STA increases, and the easier the STA discovers a WLAN.

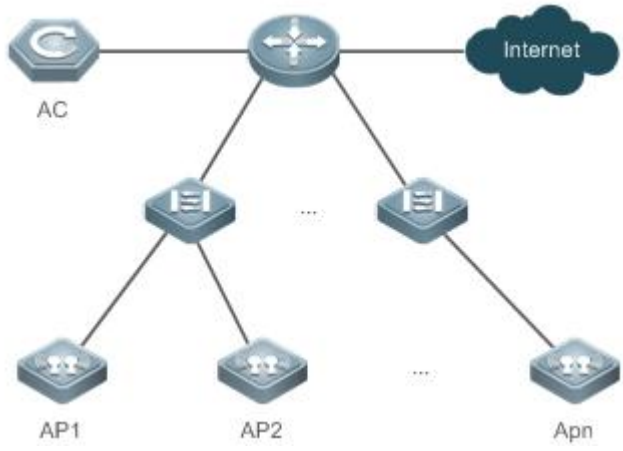
Command	**band-select scan-cycle** *value*
Parameter Description	*value*: Specifies the scanning cycle threshold of an STA, ranging from 1 to 1000 milliseconds.
Defaults	The default value is 200 milliseconds.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show band-select configuration** command to display parameters of the Band Select function.
- Run the **show running-config** command to check whether the Band Select function is enabled.
- After a period of running, run the **show band-select statistics** command to check the statistics on the AC.
- Check whether the Band Select function controls the active scanning process by capturing packets.

Configuration Example

Configuring Band Select for a WLAN Using a Fit AP Architecture

Scenario **Figure 2- 2**	 Figure 2-2 shows a typical WLAN using a fit AP architecture. - AC is a wireless access controller. - AP_1, AP_2 … AP_n are dual-band APs. - The AC and APs are connected through layer-2 switch devices and layer-3 routers. - The WLAN for which the Band Select function needs to be enabled is WLAN 99, whose SSID is wlan-bandselect. This WLAN is mapped to the two RF interfaces of all dual-band APs.
Configuration Steps	- (Optional) Configure the parameters of the Band Select function on the AC. - Enable the Band Select Function for WLAN 99 on the AC.

AC	AC# configure terminal AC(config)# wlan-config 99 AC(config-wlan)# band-select enable
Verification	Access WLAN "wlan-bandselect" by using a dual-band STA. ● The STA accesses the 5 GHz band. (The STA may also access the 2.4 GHz band upon band selection failure.) ● Check the statistics of the Band Select function on the AC. The count should increase.
AC	A# show band-select statistics Band Select Statistics Number of dual band client..... 1 Number of dual band client added..... 1 Number of dual band client expired..... 0 Number of suppressed client..... 0 Number of suppressed client added..... 0 Number of suppressed client expired..... 0

Common Errors

- The parameters are improper.
- The Band Select function is not enabled.
- One of the two RF interfaces of a dual-band AP is disabled.

2.5 Monitoring

Displaying

Description	Command
Displays the configuration of the Band Select function.	**show band-select configuration**
Displays the statistics of the Band Select function.	**show band-select statistics**

Chapter 14 WLAN Security Configuration

1. Configuring RSNA
2. Configuring WIDS

1 Configuring RSNA

1.1 Overview

The Robust Security Network Architecture (RSNA) function provides security mechanisms for WLANs.

A WLAN uses open media and public electromagnetic waves as a carrier to transmit data signals. Neither communication party is connected with a cable. If transmission links are not properly protected through encryption, data transmission will be at great risk. Therefore, security mechanisms are especially important in a WLAN.

To enhance the security, a WLAN should be provided with at least the authentication and encryption mechanisms:

- Authentication mechanism: The authentication mechanism is used to authenticate users and allow only specified users (authorized users) to use network resources.
- Encryption mechanism: The encryption mechanism is used to encrypt data on wireless links to ensure that WLAN data can be received and understood only by expected users.

Protocols and Standards

- IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements -2007
- WI-FI Protected Access – Enhanced Security Implementation Based On IEEE P802.11i Standard -Aug 2004
- 802.11i IEEE Standard for Information technology –Telecommunications and information exchange between systems –Local and metropolitan area networks – Specific requirements

1.2 Applications

Application	Description
WEP Encryption	In a small WLAN that has a lower requirement for security, static WEP encryption can be used to protect wireless data communication.
PSK Access Authentication	For small and medium-sized enterprise networks or family users, access authentication based on pre-shared keys can be used to enhance the security of WLANs.

1.2.1 WEP Encryption

Scenario

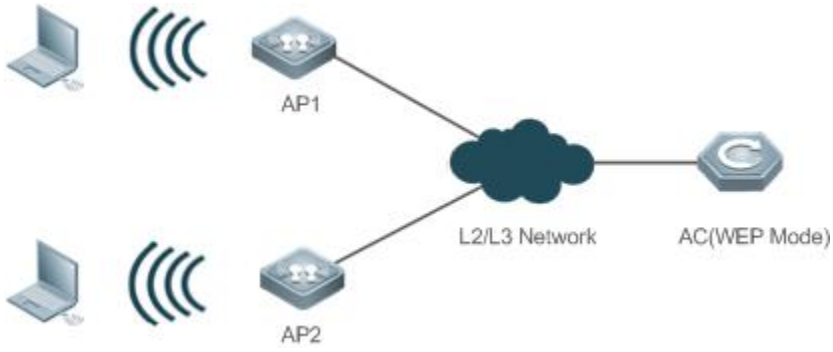
In a small WLAN that has a lower requirement for security, WEP encryption can be used.

WEP encryption can use the open-system or shared-key link authentication mode. Their differences are as follows:

- When open-system link authentication is used, WEP keys can be used only for data encryption. Even if inconsistent keys are configured, users can go online; however, data transmitted after the users go online is discarded by the receiver due to key inconsistency.
- When shared-key link authentication is used, WEP keys are used for link authentication and data encryption. If inconsistent keys are configured, link authentication fails and the client cannot go online.

Figure 1- 1 shows the scenario of static WEP encryption.

Figure 1- 1



Deployment

- Configure a WLAN on the AC.
- Configure WEP encryption in WLAN security configuration mode.
- Push the WLAN to APs.

1.2.2 PSK Access Authentication

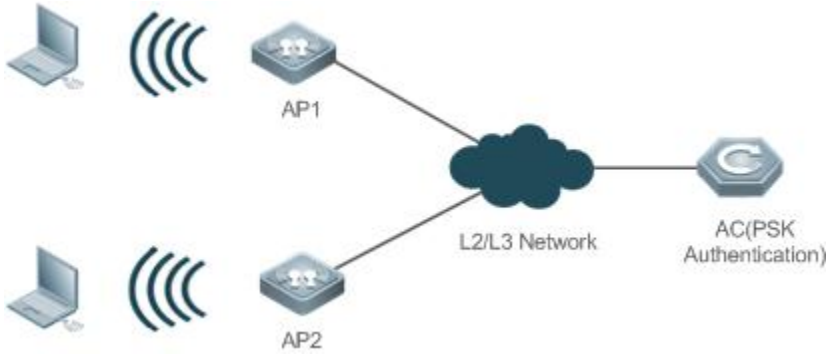
Scenario

Small and medium-sized enterprise networks or family users can use the WPA or WPA2 standard to enhance WLAN security. The simplest method is to use the pre-shared key authentication (referred to as WPA-PSK and WPA2-PSK respectively). In this case, WPA is similar to WEP, but users can achieve higher security through WPA and 802.11i, including more robust authentication and better encryption algorithms.

In PSK authentication, the same pre-shared key should be configured for an STA and an AP to establish connection and communication. No additional authentication server is required.

Figure 1- 2 shows the scenario of PSK authentication.

Figure 1- 2



Deployment

- Configure a WLAN on the AC.
- Configure PSK authentication in WLAN security configuration mode.
- Push the WLAN to APs.

- Use this authentication with WEB authentication to support web-based authentication and charging.

1.3 Features

Basic Concepts

WPA

Wi-Fi Protected Access (WPA) is a wireless security draft defined by the Wi-Fi Alliance. The IEEE802.11i standard is compatible with this draft.

RSN

The IEEE802.11i standard defines the concept of Robust Security Network (RSN): and makes many improvements against various defects of the WEP encryption mechanism. The functions are equal to WPA2 launched by the Wi-Fi Alliance.

TKIP

The Temporal Key Integrity Protocol (TKIP) is an enhancement on WEP security. TKIP provides key mixing, message integrity check and key mechanism re-generation for each packet, thus eliminating hidden risks of WEP.

AES

Advanced Encryption Standard (AES) is a new encryption standard published by the National Institute of Standards and Technology (NIST) of the United States. On October 2, 2000, the Rijndael algorithm designed by Joan Daemen and Vincent Rijmen from Belgium won with its excellent performance and anti-attack capabilities, and became the new-generation encryption standard AES.

CCMP

Counter CBC-MAC Protocol (CCMP) uses AES, which is safer than TKIP.

AKM

Authentication and Key Management (AKM) is an access authentication mode for users to access a WLAN.

Overview

Feature	Description
Link Verification	Verify the security of a wireless link before an STA associates with a WLAN.
Access Authentication	Perform authentication for an STA that accesses a WLAN.
Wireless Data Encryption	Implement security protection for communication data of an STA that accesses a WLAN.

1.3.1 Link Verification

Link verification refers to 802.11 authentication, which is a low-level authentication mechanism. Link verification is performed when an STA associates with an AP over 802.11, which is earlier than access authentication. Before accessing a WLAN, the STA must be authenticated over 802.11. 802.11 authentication marks the beginning of the handshake process when an STA accesses a WLAN and the first step for network connection.

The IEEE 802.11 standard defines two approaches to link authentication:

- Open-system link authentication

- Shared-key link authentication

Working Principle

Open-System Link Authentication

Open-system link authentication allows all users to access a WLAN. In this sense, no data protection is provided, which means that no authentication is performed. In other words, if the authentication mode is set to open-system authentication, all STAs that request authentication can pass the authentication.

Open-system link authentication comprises two steps:

Step 1: An STA requests authentication. The STA sends an authentication request that contains the ID (usually the MAC address) of the STA.

Step 2: An AP returns the authentication result. The AP sends an authentication response that contains information indicating whether the authentication succeeds or fails. If the authentication succeeds, the STA and AP pass the bidirectional authentication.

Figure 1- 5

Shared-key Link Authentication

Shared-key link authentication is another authentication mechanism in addition to the open-system link authentication. Shared-key link authentication requires that the same shared key be configured for an STA and an AP. The shared-key link authentication can be configured only in static WEP encryption whereas the open-system link authentication is available in all the other modes.

The process of shared-key link authentication is as follows:

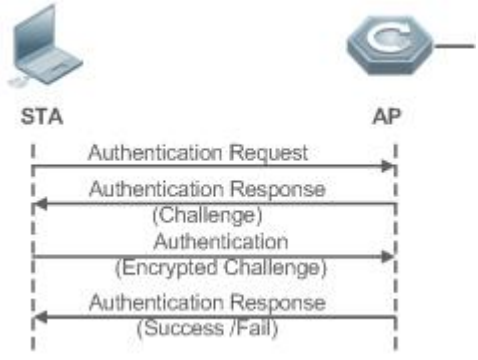
Step 1: An STA sends an authentication request to an AP.

Step 2: The AP generates a Challenge packet (a string) at random and sends the packet to the STA.

Step 3: The STA copies the received string to a new message, encrypts the message with a key and then sends the encrypted message to the AP.

Step 4: After receiving the message, the AP decrypts the message with the key, and then compares the decrypted string with the string sent to the STA. If the two strings are the same, it indicates that the STA has the same shared key as that on the AP and the shared-key authentication succeeds; otherwise, the shared-key authentication fails.

Figure 1- 6



1.3.2 Access Authentication

Access authentication is a solution that enhances WLAN security.

After an STA is associated with an AP, whether the STA can use the service provided by the AP depends on the result of access authentication. If the STA passes the authentication, the AP enables the logical port for the STA; otherwise, the STA is not allowed to access the WLAN.

The IEEE 802.11 standard defines the following authentication:

- PSK access authentication

Working Principle

PSK Access Authentication

Pre-shared Key (PSK) is an 802.11i authentication mode, which performs authentication with pre-defined static keys. This authentication approach requires that an STA and an AP be configured with the same pre-shared key. If their keys are the same, the PSK access authentication succeeds; otherwise, the PSK access authentication fails.

1.3.3 Wireless Data Encryption

Compared with a wired network, a wireless network is prone to greater security risks. Within an area, all WLAN devices share the same transmission medium and any device can receive data from all the other devices. This feature poses threat to WLAN data.

The IEEE 802.11i protocol defines the following encryption algorithms:

- WEP encryption
- TKIP encryption
- AES encryption

Working Principle

WEP Encryption

Wired Equivalent Privacy (WEP) is a data encryption mode specified in the original IEEE 802.11 standard, and is the basis for WLAN security authentication and encryption. WEP is used to promote the privacy of data exchanged between authorized users in a WLAN and prevent the data from being stolen.

WEP uses the RC4 algorithm to promote data privacy and implements authentication by using a shared key. WEP does not specify a key management scheme. Generally, keys are configured and maintained manually. WEP that does not provide a key distribution mechanism is called manual WEP or static WEP.

A WEP encrypted key may contain 64 bits or 128 bits. The 24-bit Initialization Vector (IV) is generated by the system. Therefore, a shared key to be configured on an AP and an STA consists of only 40 bits or 104 bits. In practice, the 104-bit WEP keys are widely used to replace the 40-bit WEP keys. WEP using 104-bit keys are called WEP-104. Although WEP-104 increases the security of WEP encryption, WEP encryption is prone to security risks due to limitations of the RC encryption algorithm and statically configured keys. WEP encryption cannot ensure the confidentiality and integrity of data or access authentication.

TKIP Encryption

Temporal Key Integrity Protocol (TKIP) is a temporary makeshift solution created by the IEEE 802.11 organization for fixing the WEP encryption mechanism. Like WEP encryption, TKIP encryption also uses the RC4 algorithm. But compared with WEP encryption, TKIP encryption can provide much safer protection for WLAN services in the following aspects:

A static WEP key is manually configured and all users within the same service area share the same key. A TKIP key is generated through dynamic negotiation, and each packet has a unique key.

– TKIP increases the key length from 40 bits to 128 bits, and the IV length from 24 bits to 48 bits, thus improving the security of WEP encryption.

– TKIP supports Message Integrity Check (MIC) and the replay prevention function.

AES Encryption

The Counter mode with CBC-MAC Protocol (AES-CCMP) is the most advanced wireless security protocol oriented to the public.

The IEEE 802.11i standard requires that CCMP be used to provide four security services, namely, authentication, confidentiality, integrity, and replay prevention. CCMP uses the 128-bit Advanced Encryption Standard (AES) to implement confidentiality and uses the CBC-MAC to ensure data integrity and authentication.

As a new advanced encryption standard, AES uses the symmetrical block encryption technology to provide better encryption performance than the RC4 algorithm in WEP/TKIP. It is the new-generation encryption technology that replaces WEP and brings more powerful security protection for WLANs.

1.4 Configuration

Configuration	Description and Command	
Configuring Static WEP	(Mandatory) It is used to enable static WEP encryption.	
	security static-wep-key encryption	Enables static WEP for a WLAN and configures a static WEP key.
	(Optional) It is used to configure the link authentication mode.	
	security static-wep-key authentication	Configures the link authentication mode of static WEP.
Configuring WPA Authentication	(Mandatory) It is used to enable WPA authentication.	
	security wpa	Configures WPA authentication.
	security wpa ciphers	Configures the encryption mode of WPA authentication.
	security wpa akm	Configures the access authentication mode for WPA authentication.
	(Optional) It is used to configure a shared key for WPA PSK authentication.	
	security wpa akm psk set-key	Configures a shared key for WPA PSK authentication.
Configuring RSN	(Mandatory) It is used to enable RSN authentication.	

Configuration	Description and Command	
Authentication	**security rsn**	Configures RSN authentication.
	security rsn ciphers	Configures the encryption mode for RSN authentication.
	security rsn akm	Configures the access authentication mode for RSN authentication.
	(Optional) It is used to configure a shared key for RSN PSK authentication.	
	security rsn akm psk set-key	Configures a shared key for RSN PSK authentication.
Configuring MAB Authentication	(Optional) It is used to configure MAB authentication.	
	dot1x-mab	Enables MAB authentication.
Configuring Authentication Parameters	(Optional) It is used to configure key interaction parameters and the jitter prevention time in WEB authentication.	
	authtimeout forbidcount	Configures the association forbidding count after four-way handshake key interaction fails.
	authtimeout forbidtime	Configures the association forbidding interval after four-way handshake key interaction fails.
	authtimeout groupcount	Configures the multicast key negotiation packet re-transmission count.
	authtimeout grouptime	Configures the timeout duration of multicast key negotiation packets.
	authtimeout paircount	Configures the uncast key negotiation packet re-transmission count.
	authtimeout pairtime	Configures the timeout duration of unicast key negotiation packets.
	webauth prevent-jitter	Configures the jitter prevention time of WEB authentication.

1.4.1 Configuring Static WEP

Configuration Effect

- Enable static WEP encryption and provide WEP encryption protection for WLAN data.
- Configure the link authentication mode.

Notes

- The link authentication mode must be configured after static WEP encryption is enabled.
- In the security mode of a WLAN, static WEP encryption cannot be configured together with other authentication encryption.
- Only one WLAN can be configured with static WEP encryption

Configuration Steps

Enabling Static WEP

- Mandatory.
- Enable static WEP encryption in WLAN security configuration mode on the AC.

Command	**security static-wep-key encryption** *key-length* { **ascii** | **hex** } *key-index key*
Parameter Description	*key-length*: Specifies the key length, which can be 40 bits or 104 bits. **ascii**: Specifies that the WEP key is ASCII code. **hex**: Specifies that the WEP key is hexadecimal code. *key-index*: Specifies the key index, ranging from 1 to 4. *Key*: Specifies key data.
Defaults	Static WEP is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	This command is used to configure a static WEP key and enable static WEP. This command can be configured repeatedly, but only the last configuration takes effect. The key length must be the same as the *key-length* parameter in the command.

Configuring the Link Authentication Mode

- (Optional) The default link authentication mode is open-system link authentication. This command can be used to configure shared-key link authentication.
- Enable static WEP encryption in security configuration mode on the AC.
- The link authentication mode can be configured only after static WEP encryption is enabled. After configuring the sharedkey link authentication mode, set the link authentication mode to shared key link authentication on the STA; otherwise, the STA cannot access the WLAN.

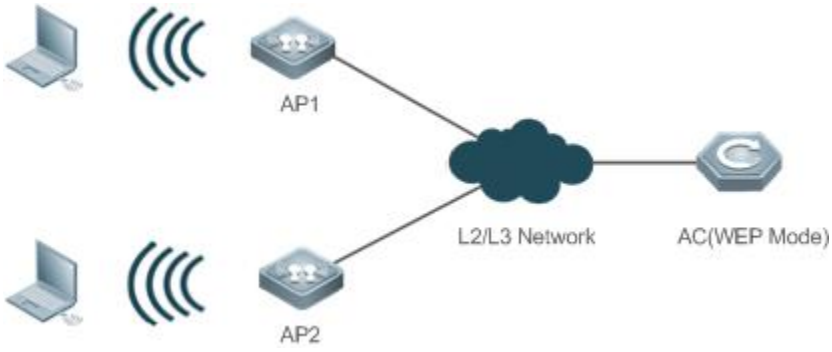
Command	**security static-wep-key authentication** { **open** | **share-key** }
Parameter Description	**open**: Configures open-system link authentication. **share-key**: Configures shared key link authentication.
Defaults	An STA accesses a WLAN by using open-system link authentication by default.
Command Mode	WLAN security configuration mode
Usage Guide	Configure the link authentication mode after configuring a static WEP key. The link authentication mode cannot be configured for other security configuration modes than static WEP.

Verification

Run the **show running-config** | **begin wlansec** *wlan_id* command to check whether the configuration takes effect.

Configuration Example

Configuring Static WEP Encryption and Using Shared-Key Link Authentication for WLAN 1

Scenario Figure 1-7	 In a Fit AP environment, configure WLAN 1 on the AC and configure the security policies 1 as follows: 1. Enable static WEP encryption. 2. Configure shared-key link authentication.
Configuration Steps	● Access the security configuration mode of WLAN 1. ● Enable static WEP encryption and configure a WEP key. ● Set the link authentication mode to shared-key link authentication.
AC	FS(config)#wlansec 1 FS(config-wlansec)#security static-wep-key encryption 40 ascii 1 12345 FS(config-wlansec)#security static-wep-key authentication share-key
Verification	Run the **show running-config | begin wlansec** *wlan_id* command to check whether the configuration takes effect.
AC	FS#show running-config | begin wlansec 1 wlansec 1 security static-wep-key encryption 40 ascii 1 12345 security static-wep-key authentication share-key !

Common Errors

- The configured key length is inconsistent with the specified key length.
- Static WEP is configured for multiple WLANs.
- The link authentication mode is configured before static WEP is enabled.

1.4.2 Configuring WPA Authentication

Configuration Effect

- Enable WPA authentication for a WLAN.
- Specify the access authentication mode and encryption mode in WPA authentication.

Notes

- When WPA authentication is used, the encryption mode and access authentication mode must also be configured.
- If the access authentication mode is set to PSK, a PSK key must be configured.
- In the security mode of a WLAN, WPA authentication cannot be configured with WEP authentication.

Configuration Steps

Configuring WPA Authentication

- Mandatory.
- Enable WPA authentication in WLAN security configuration mode on the AC.

Command	**security wpa** { **enable** | **disable** }
Parameter Description	**enable**: Enables WPA authentication. **disable**: Disables WPA authentication.
Defaults	WPA authentication is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	The encryption mode and access authentication mode can be configured in WPA authentication only after WPA authentication is enabled; otherwise, the configuration does not take effect. When WPA authentication is used, the encryption mode and access authentication mode must also be configured. If either the encryption mode or the access authentication mode is configured or neither of them is configured, STAs cannot access a WLAN.

Configuring the Encryption Mode of WPA Authentication

- Mandatory.
- It is configured in WLAN security configuration mode on the AC.
- The encryption mode of WPA authentication can be configured only after WPA authentication is enabled. The AES and TKIP encryption modes can be enabled at the same time in WLAN security configuration mode. After an encryption mode is configured for a WLAN, communication data between an STA and the WLAN is protected by the corresponding encryption mode.

Command	**security wpa ciphers** { **aes** | **tkip** } { **enable** | **disable** }
Parameter Description	**aes**: Configures the AES encryption mode. **tkip**: Configures the TKIP encryption mode. **enable**: Enables the encryption mode of WPA authentication. **disable**: Disables the encryption mode of WPA authentication.
Defaults	No encryption mode is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	This command is used to enable an encryption mode of WPA authentication, which can be AES or TKIP. The AES and TKIP encryption modes can be enabled at the same time in WLAN security configuration mode.

Configuring the Access Authentication Mode of WPA authentication

- Mandatory.

- It is configured in WLAN security configuration mode on the AC.
- The access authentication mode can be configured only after WPA authentication is enabled. Only one access authentication mode can be enabled for a WLAN in security configuration mode. An STA can access a WLAN that is enabled with access authentication only after passing the access authentication.

Command	**security wpa akm psk** { **enable** | **disable** }
Parameter Description	**psk**: Sets the access authentication mode to pre-shared key authentication. **enable**: Enables the access authentication mode of WPA authentication. **disable**: Disables the access authentication mode of WPA authentication.
Defaults	No access authentication mode is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	The access authentication mode can be configured only after WPA authentication is enabled. Only one access authentication mode can be enabled for a WLAN in security configuration mode.

Configuring a Shared Key for WPA Authentication

- (Optional) It must be configured when WPA PSK authentication is enabled.
- It is configured in WLAN security configuration mode on the AC.

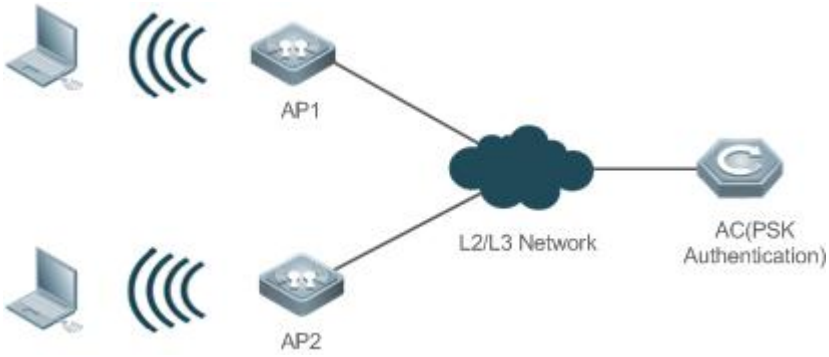
Command	**security wpa akm psk set-key** { **ascii** *ascii-key* / **hex** *hex-key* }
Parameter Description	**ascii**: Specifies that the PSK key is ASCII code. *ascii-key*: Specifies a key in the ASCII format, consisting of 8 to 63 ASCII characters. **hex**: Specifies that the PSK key is hexadecimal code. *hex-key*: Specifies a key in the hexadecimal format, consisting of 64 characters.
Defaults	N/A
Command Mode	WLAN security configuration mode
Usage Guide	This shared key takes effect only when PSK authentication is enabled. A key in the ASCII format consists of 8 to 63 characters. A key in the hexadecimal format consists of 64 characters.

Verification

Run the **show running-config** | **begin wlansec** *wlan_id* command to check whether the configuration takes effect.

Configuration Example

Configuring WPA PSK Authentication, AES Encryption and Key 12345678 for WLAN 1

Scenario **Figure 1-8**	 In a Fit AP environment, configure the security policies of WLAN 1 on the AC as follows: 1. Configure WPA PSK authentication. 2. Configure the AES encryption mode. 3. Configure the shared key 12345678.
Configuration Steps	● Access security configuration mode of WLAN 1. ● Enable WPA authentication. ● Configure the AES encryption mode for WPA authentication. ● Configure the PSK access authentication mode for WPA authentication. ● Configure the PSK key 12345678.
AC	FS(config)#wlansec 1 FS(config-wlansec)#security wpa enable FS(config-wlansec)#security wpa ciphers aes enable FS(config-wlansec)#security wpa akm psk enable FS(config-wlansec)#security wpa akm psk set-key ascii 12345678
Verification	Run the **show running-config** | **begin wlansec** *wlan_id* command to check whether the configuration takes effect.
AC	FS#show running-config | begin wlansec 1 wlansec 1 security wpa enable security wpa ciphers aes enable security wpa akm psk enable security wpa akm psk set-key ascii 12345678 !

Common Errors

- The WLAN has been enabled with other encryption and authentication modes (such as WEP).
- A WPA encryption mode is configured before WPA authentication is enabled in WLAN security configuration mode.
- An access authentication mode is configured before WPA authentication is enabled in WLAN security configuration mode.

- If an access authentication mode is enabled in WLAN security configuration mode, no other access authentication mode can be configured.
- A WPA PSK key is configured before WPA authentication is enabled.
- The ASCII key consists of less than 8 characters or more than 63 characters.
- The hexadecimal key does not consist of 64 characters.

1.4.3 Configuring RSN Authentication

Configuration Effect

- Enable RSN authentication for a WLAN.
- Specify the access authentication mode and encryption mode in RSN authentication.

Notes

- When RSN authentication is used, the encryption mode and access authentication mode must also be configured.
- If the access authentication mode is set to PSK, a PSK key must be configured.
- In the security mode of a WLAN, RSN authentication cannot be configured with WEP authentication.

Configuration Steps

Configuring RSN Authentication

- Mandatory.
- Enable RSN authentication in WLAN security configuration mode on the AC.

Command	**security rsn** { **enable** | **disable** }
Parameter Description	**enable**: Enables RSN authentication. **disable**: Disables RSN authentication.
Defaults	RSN authentication is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	The encryption mode and access authentication mode can be configured in RSN authentication only after RSN authentication is enabled; otherwise, the configuration does not take effect. When RSN authentication is used, the encryption mode and access authentication mode must also be configured. If either the encryption mode or the access authentication mode is configured or neither of them is configured, STAs cannot access a WLAN.

Configuring the Encryption Mode for RSN Authentication

- Mandatory.
- It is configured in WLAN security configuration mode on the AC.
- The encryption mode in RSN authentication can be configured only after RSN authentication is enabled. The AES and TKIP encryption modes can be enabled at the same time in WLAN security configuration mode. After an encryption mode is configured for a WLAN, communication data between an STA and the WLAN is protected by the corresponding encryption mode.

Command	**security rsn ciphers** { **aes** | **tkip** } { **enable** | **disable** }
Parameter Description	**aes**: Configures the AES encryption mode. **tkip**: Configures the TKIP encryption mode. **enable**: Enables the encryption mode for RSN authentication. **disable**: Disables the encryption mode for RSN authentication.
Defaults	No encryption mode is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	This command is used to enable an encryption mode for RSN authentication, which can be AES or TKIP. The AES and TKIP encryption modes can be enabled at the same time in WLAN security configuration mode.

Configuring the Access Authentication Mode for RSN Authentication

- Mandatory.
- It is configured in WLAN security configuration mode on the AC.
- The access authentication mode in RSN authentication can be configured only after RSN authentication is enabled. Only one access authentication mode can be enabled for a WLAN in security configuration mode. An STA can access a WLAN that is enabled with access authentication only after passing the access authentication.

Command	**security rsn akm psk** { **enable** | **disable** }
Parameter Description	**psk**: Sets the access authentication mode to pre-shared key authentication. **enable**: Enables the access authentication mode for RSN authentication. **disable**: Disables the access authentication mode for RSN authentication.
Defaults	No access authentication mode is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	The access authentication mode can be configured only after RSN authentication is enabled. Only one access authentication mode can be enabled for a WLAN in security configuration mode.

Configuring a Shared Key for RSN Authentication

- (Optional) It must be configured when RSN PSK authentication is enabled.
- It is configured in WLAN security configuration mode on the AC.

Command	**security rsn akm psk set-key** { **ascii** *ascii-key* | **hex** *hex-key* }
Parameter Description	**ascii**: Specifies that the PSK key is ASCII code. *ascii-key*: Specifies a key in the ASCII format, consisting of 8 to 63 ASCII characters. **hex**: Specifies that the PSK key is hexadecimal code. *hex-key*: Specifies a key in the hexadecimal format, consisting of 64 characters.
Defaults	N/A
Command Mode	WLAN security configuration mode
Usage Guide	This shared key takes effect only when PSK authentication is enabled.

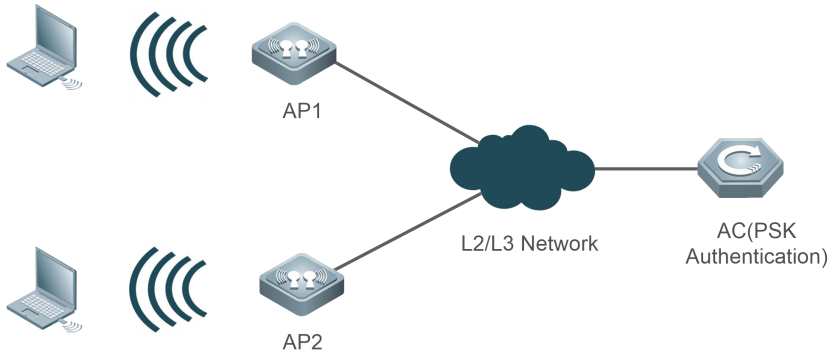
	A key in the ASCII format consists of 8 to 63 characters. A key in the hexadecimal format consists of 64 characters.

Verification

Run the **show running-config | begin wlansec** *wlan_id* command to check whether the configuration takes effect.

Configuration Example

Configuring RSN PSK Authentication, AES Encryption and Key 12345678 for WLAN 1

Scenario **Figure 1-9**	 In a Fit AP environment, configure the security policies of WLAN 1 on the AC as follows: 1. Configure RSN PSK authentication. 2. Configure the AES encryption mode. 3. Configure the shared key to 12345678.
Configuration Steps	● Access security configuration mode of WLAN 1. ● Enable RSN authentication. ● Configure the AES encryption mode for RSN authentication. ● Configure the PSK access authentication mode for RSN authentication. ● Configure the PSK key 12345678.
AC	FS(config)#wlansec 1 FS(config-wlansec)#security rsn enable FS(config-wlansec)#security rsn ciphers aes enable FS(config-wlansec)#security rsn akm psk enable FS(config-wlansec)#security rsn akm psk set-key ascii 12345678
Verification	Run the **show running-config	begin wlansec** *wlan_id* command to check whether the configuration takes effect.
AC	FS#show running-config | begin wlansec 1 wlansec 1 security rsn enable security rsn ciphers aes enable

	security rsn akm psk enable security rsn akm psk set-key ascii 12345678 !

Common Errors

- The WLAN has been enabled with other encryption and authentication modes (such as WEP).
- An RSN encryption mode is configured before RSN authentication is enabled in WLAN security configuration mode.
- An access authentication mode is configured before RSN authentication is enabled in WLAN security configuration mode.
- If an access authentication mode is enabled in WLAN security configuration mode, no other access authentication mode can be configured.
- An RSN PSK key is configured before RSN authentication is enabled.
- The ASCII key consists of less than 8 characters or more than 63 characters.
- The hexadecimal key does not consist of 64 characters.

1.4.4 Configuring Authentication Parameters

Configuration Effect

- Configure key interaction parameters.
- Configure the jitter prevention time in WEB authentication.

Notes

- The jitter prevention time in WEB authentication can be configured only after WEB authentication is enabled.

Configuration Steps

Configuring Key Interaction Parameters

- Optional. Generally, it is unnecessary to configure key interaction parameters. It is recommended to set the packet re-transmission count and timeout duration to great values for a poor WLAN environment.
- It is configured in WLAN security configuration mode on the AC.

Command	**authtimeout** { **forbidcount** *count* | **forbidtime** *time* | **groupcount** *count* | **grouptime** *timeout* | **paircount** *count* | **pairtime** *timeout* }
Parameter Description	**forbidcount** *count*: Configures the association forbidding count after four-way handshake key interaction fails. **forbidtime** *time*: Configures the association forbidding interval after four-way handshake key interaction fails. **groupcount** *count*: Configures the multicast key negotiation packet re-transmission count. **grouptime** *timeout*: Configures the timeout duration of multicast key negotiation packets. **paircount** *count*: Configures the unicast key negotiation packet re-transmission count. **pairtime** *timeout*: Configures the timeout duration of unicast key negotiation packets.
Defaults	The association forbidding count after four-way handshake key interaction fails is 10. The association forbidding interval after four-way handshake key interaction fails is 5 seconds. The default multicast key negotiation packet re-transmission count is 7.

	The default timeout duration of multicast key negotiation packets is 1200 ms. The default unicast key negotiation packet re-transmission count is 7. The default timeout duration of unicast key negotiation packets is 1200 ms.
Command Mode	WLAN security configuration mode
Usage Guide	Key interaction parameters take effect only in PSK authentication.

Configuring the Jitter Prevention Time of WEB Authentication

- Optional. The default jitter prevention time of WEB authentication is 300 seconds. Users can configure the jitter prevention time based on actual requirements or disable the jitter prevention of WEB authentication by setting the time to 0 seconds.
- It is configured in WLAN security configuration mode on the AC.

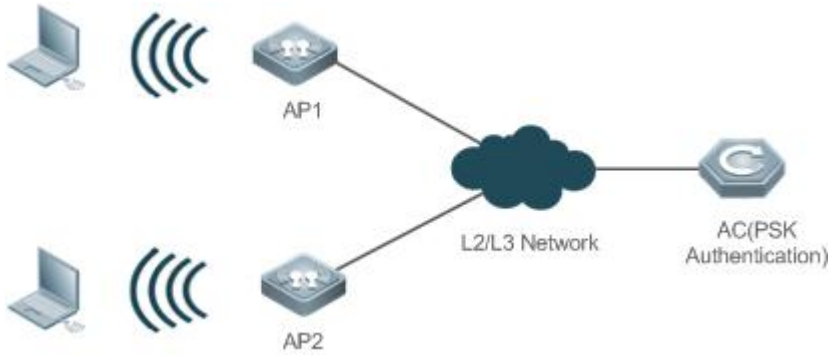
Command	**webauth prevent-jitter** *timeout*
Parameter Description	*timeout*: Configures the jitter prevention time of WEB authentication, ranging from 0 to 86400 seconds (the jitter prevention of WEB authentication is disabled when this parameter is set to 0).
Defaults	The default jitter prevention time of WEB authentication is 300 seconds.
Command Mode	WLAN security configuration mode
Usage Guide	The jitter prevention time of WEB authentication can be configured only after WEB authentication is enabled.

Verification

Run the **show running-config | begin wlansec** *wlan_id* command to check whether the configuration takes effect.

Configuration Example

Configuring the RSN-PSK + WEB Authentication Mode, the Unicast Key Negotiation Re-transmission Count to 5, and the Jitter Prevention Time of WEB Authentication to 900 Seconds for WLAN 1

Scenario **Figure 1-12**	 In a Fit AP environment, configure the security policies of WLAN 1 on the AC as follows: 1. Configure RSN PSK authentication. 2. Enable WEB authentication.
Configuration Steps	● Access the security configuration mode of WLAN 1. ● Enable RSN authentication. ● Configure the AES encryption mode for RSN authentication.

	● Configure the PSK access authentication mode for RSN authentication. ● Configure the PSK key 12345678. ● Set the unicast key negotiation packet re-transmission count to 5. ● Configure WEB authentication. ● Set the jitter prevention time of WEB authentication to 900 seconds.
AC	FS(config)#wlansec 1 FS(config-wlansec)#security rsn enable FS(config-wlansec)#security rsn ciphers aes enable FS(config-wlansec)#security rsn akm psk enable FS(config-wlansec)#security rsn akm psk set-key ascii 12345678 FS(config-wlansec)#authtimeout paircount 5 FS(config-wlansec)#webauth FS(config-wlansec)#webauth prevent-jitter 900
Verification	Run the **show running-config** | **begin wlansec** *wlan_id* command to check whether the configuration takes effect.
AC	FS#show running-config | begin wlansec 1 wlansec 1 security rsn enable security rsn ciphers aes enable security rsn akm psk enable security rsn akm psk set-key ascii 12345678 webauth prevent-jitter 900 webauth authtimeout paircount 5

Common Errors

- The jitter prevention time of WEB authentication is configured before WEB authentication is enabled.

1.5 Monitoring

Displaying

Description	Command
Displays security configuration of a WLAN.	**show wlan security** *wlan-id*
Displays security configuration of an STA.	**show wclient security** *mac-address*

2 Configuring WIDS

2.1 Overview

Compared with wired networks, Wireless LAN (WLAN) has unparalleled advantages, such as convenient deployment, flexible use, efficient cost, and easy extension, making it more and more prevalent. However, for the openness of its channels, WLAN is much vulnerable to various network threats, such as rogue access points (APs), Ad-hoc networks, and all types of protocol attacks. Therefore, security becomes a major factor that hinders WLAN development.

Wireless Intrusion Detection System (WIDS) detects vicious STA attacks and invasions in the early stage, which helps network administrators actively observe and defend against the hidden dangers in networks in the first time.

2.2 Applications

Application	Description
Frame Filtering	Facing illegal STAs attempting to access WLAN, WIDS frame filtering helps control STA access.
User Isolation	Facing an STA intending to visit other STAs in WLAN, WIDS user isolation helps isolate their direct communication.
IDS	Facing all kinds of invasion attacks in WLAN, Intrusion Detection System (IDS) helps detect those attacks.
Rogue Detection and Containment	Illegal or rogue devices in WLAN jeopardize STAs and normal services by faking services. Facing it, Rogue detection and containment help monitor and contain them.

2.2.1 Frame Filtering

Scenario

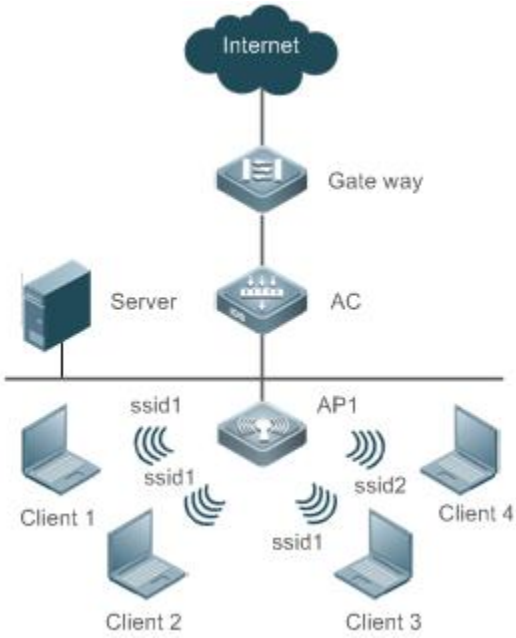
The wireless access control service is provided in WLAN, including allowing specified STAs to access WLAN or specified networks, forbidding STAs from accessing WLAN or specified networks, forbidding low-rate stations (STAs) from accessing WLAN, as well as dynamically controlling network access.

The figure below is an example, assuming that there are the following deployment requirements in the network:

- Allow Client 1 to access WLAN and Client 2 to access SSID 1.
- Prohibit Client 3 from accessing WLAN and Client 4 from accessing SSID 2.
- Filter and kick out low-rate STAs.
- Dynamically control STA access.

The networking topology is shown as follows:

Figure 1- 1 Networking Topology of Wireless Access Control



Deployment

The key configuration points for the devices are:

- Add Client 1 to a WIDS whitelist. As a result, Client 1 can access the WLAN service provided by all APs under the AC. Other STAs not in the list cannot.
- Add Client 2 to the SSID 1-based whitelist. As a result, Client 2 can access SSID 1 provided by all APs under the AC. Other STAs not in the list cannot.
- Add Client 3 to a static blacklist. As a result, Client 3 cannot access the WLAN service provided by all APs under the AC.
- Add Client 4 to the SSID 1-based blacklist. As a result, Client 4 cannot access SSID 1 provided by all APs under the AC.
- Configure the low-rate threshold. STAs of an AC with rates less than the threshold will be kicked out.
- Enable the dynamic blacklist function, supporting the IDS function. After the dynamic blacklist function is enabled, any detected attack will be added into the dynamic blacklist. When the blacklist is within aging duration, the listed STAs will continue to be forbidden from communication accessed by the current AP.

2.2.2 User Isolation

Scenario

Layer-2 user isolation is provided in WLAN, including AP-based, AP-SSID based, AC-based, AC-SSID based, and SSID-based.

Assuming there are the following deployment requirements in the network:

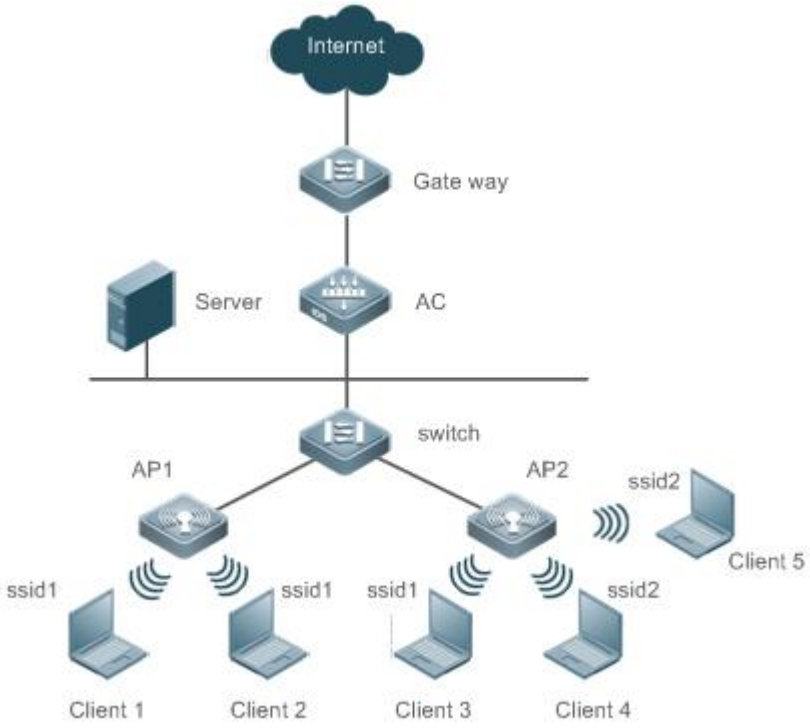
Client 1 to Client 3 are associated with SSID 1, and Client 4 and Client 5 are associated with SSID 2. SSID 1 and SSID 2 are mapped to the same VLAN. Client 1 to Client 5 are layer-2 users.

- Direct communication cannot be conducted between Client 1 and Client 2, and among Client 3 to Client 5, but can be done among other users.
- Direct communication cannot be conducted between Client 1 and Client 2, and between Client 4 and Client 5, but can be done among other users.

- Direct communication cannot be conducted between Client 1 and Client 3, Client 4 or Client 5, and between Client 2 and Client 3, Client 4 or Client 5, but can be done among other users.
- Direct communication cannot be conducted between Client 3 and Client 1 or Client 2, but can be done among other users.
- Direct communication cannot be conducted among Client 1 to Client 3, but can be done among other users.

The networking topology is shown as follows:

Figure 1- 2 Networking Topology of Wireless User Isolation



Deployment

The key configuration points for the devices are:

- Configure AP-based user isolation. As a result, direct communication cannot be conducted between Client 1 and Client 2, and among Client 3 to Client 5.
- Configure AP-SSID based user isolation. As a result, direct communication cannot be conducted between Client 1 and Client 2, and between Client 4 and Client 5.
- Configure AC-based user isolation. As a result, direct communication cannot be conducted between Client 1 or Client 2 and Client 3 to Client 5.
- Configure AC-SSID based user isolation. As a result, direct communication cannot be conducted between Client 3 and Client 1 or Client 2.
- Configure SSID 1-based user isolation. As a result, direct communication cannot be conducted among Client 1, Client 2 and Client 3.

2.2.3 IDS

Scenario

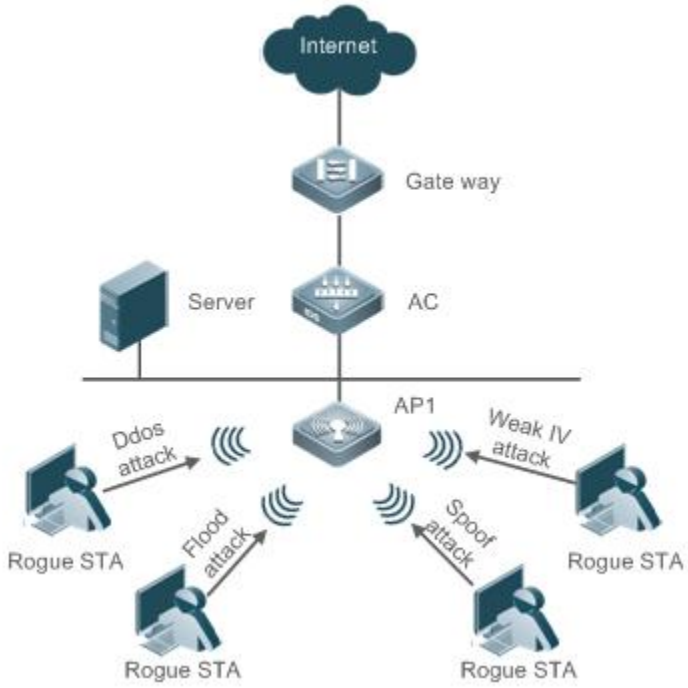
Wireless invasion attacks exist in networks, including Distributed Denial of Service (DDoS), spoofing, flooding, and Weak IV attacks. It requires APs to detect these attacks and carry out countermeasures.

Assuming there are the following deployment requirements in the network:

- DDoS attacks
- Spoofing attacks
- Flooding attacks
- Weak IV attacks

The networking topology is shown as follows:

Figure 1- 3 Networking Topology of IDS



Deployment

The key configuration points for the devices are:

- Enable DDoS detection with thresholds specified which perform statistics of ARP, SYN and ICMP attack packets. If any threshold is exceeded, the detection results will be logged, and the users will be blacklisted if the dynamic blacklist is enabled.
- Enable the spoofing detection with related thresholds specified to detect the deauthentication and disassociation packets. If any threshold is exceeded, the detection results will be logged, and the users will be blacklisted if the dynamic blacklist is enabled.
- Enable flooding detection with related thresholds specified to detect the Authentication, Association, Reassociation, Deauthentication, Disassociation, Probe, Null data and Action packets. If any threshold is exceeded, the detection results will be logged, and the users will be blacklisted if the dynamic blacklist is enabled.
- Enable the Weak IV detection with related thresholds specified to detect the IV value of the Web packets. If the number of continuous attacks exceeds the threshold, the detection results will be logged, and the users will be blacklisted if the dynamic blacklist is enabled.

2.2.4 Rogue Detection and Containment

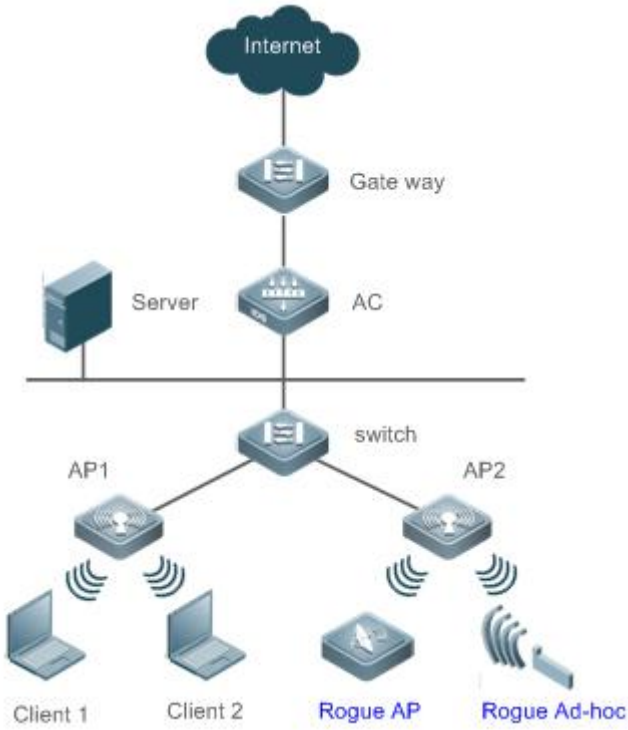
Scenario

Assuming there is the following deployment requirement in the network:

- Rogue AP and Ad-hoc devices exist in network, and detection and containment are required.

The networking topology is shown as follows:

Figure 1- 4 Networking Topology of Rogue Detection and Containment



Deployment

The key configuration points for devices are:

- Enable the Monitor or Hybrid mode for a specified AP, and start the detection timer of the AP and obtain detected data at the end of each period.
- Enable the device containment and configure the mode.
- Counter the Rogue APs and Ad-hoc devices regularly based on the containment mode and detected data, preventing users from associating with fake services.
- Before the configured AP containment takes effect, confirm that WLAN is available for the AP; otherwise, the containment function will lose effect.

2.3 Features

Basic Concepts

↘ **Working Modes**

The WIDS has the following working modes:

- Normal mode, providing only the access service
- Monitor mode, providing only the monitoring service
- Hybrid mode, providing both monitoring and access services

IDS Detection Types

The IDS attack detection has the following five types:

- DDoS attack detection, detecting DDoS attacks involving ARP, ICMP and SYN packets
- Flooding attack detection, detecting the flooding attacks involving single-user or multi-user management packets
- Spoofing attack detection, detecting the broadcast disassociation and deauthentication attacks
- Weak IV attack detection, detecting weak vector attacks
- CMCC DoS attack detection

User Isolation Modes

The user isolation has the following five modes:

- AC-based: Communication cannot proceed between layer-2 users of different APs under the same AC.
- AP-based: Communication cannot proceed between layer-2 users under the same AP.
- AC-SSID based: Communication cannot proceed between layer-2 users of different APs under the same AC and in the same WLAN.
- AP-SSID based: Communication cannot proceed between layer-2 users under the same AP and in the same WLAN.
- SSID-based: Communication cannot proceed between layer-2 users in specified WLAN.

Rogue Containment Modes

The Rogue containment has the following four modes:

- Ad-hoc containment mode, containing the Rogue Ad-hoc devices
- Rogue containment mode, containing the Rogue devices with over-limit RSSI
- SSID containment mode, containing illegal devices with the same SSID
- Config containment mode, containing the illegal devices in the static attack list or the SSID blacklist

Detected Devices

The types of detected rogue devices are as follows:

- APs
- Ad-hoc devices
- Unknown STAs

Overview

Feature	Description

Frame filtering	Certain filtering rules are used to filter the packets from STAs for access control.
IDS	Timely discovers and defends against malicious or unintentional attacks in WLAN.
User isolation	Interdicts the insecure access between STAs in WLAN to prevent disclosure of private information.
Rogue detection and containment	Monitors abnormal devices in the whole WLAN, helping the network administrators find hidden dangers in networks. Rogue containment refers to containing Rogue devices by sending fake deauthentication frames to the addresses of Rogue devices in a blacklist.

2.3.1 Frame Filtering

The access control over STAs includes: low-rate filter, whitelist, static blacklist, dynamic blacklist, SSID-based whitelist and SSID-based blacklist.

Working Principle

- **Low-Rate Filter**

The low-rate filter sets a kickout threshold. When the threshold is larger than 0, the filter is enabled. If the STA rate is lower than this threshold, the STA's packets will be discarded and this STA will be disconnected.

- **Whitelist**

The whitelist includes MAC addresses of admitted STAs. If the whitelist function is enabled, only the whistlisted can access the WLAN. Other STAs' packets will be discarded by the AP, so as to reduce the impact of illegal packets in the WLAN.

- **Static Blacklist**

The static blacklist includes MAC address of the denied STAs. If the static blacklist function is enabled, packets of STAs in the blacklist will be discarded by the AP.

- **Dynamic Blacklist**

The dynamic blacklist includes MAC addresses of the denied STAs. You can configure the dynamic blacklist if DDoS attacks are detected. For example, add the MAC address of a detected attacker into the blacklist dynamically to forbid receiving any packet from it, thereby ensuring WLAN security.

- **SSID-based Whitelist**

The SSID-based whitelist includes MAC addresses of the STAs admitted into a WLAN with a specified SSID. You can configure the SSID-based whitelist. If the SSID-based whitelist function is enabled, only the STAs in the whitelist of the specified WLAN are allowed to access. Other STAs' packets will be discarded by the AP, so as to reduce the impact of illegal packets in WLAN.

- **SSID-based Blacklist**

The SSID-based blacklist includes MAC addresses of the STAs denied by a WLAN with a specified SSID. You can configure the SSID-based blacklist. If the SSID-based blacklist function is enabled, packets of STAs in the blacklist will be discarded by the AP.

2.3.2 IDS

In order to timely find and defend against malicious or unintentional attacks in WLAN, IDS supports the detection on multiple attacks. When an attack is detected, an alert or a log will be generated to remind the network administrator of treatment. Based on detected results, the network administrator can timely adjust network configuration to clear the insecure factors in WLAN.

Currently, our devices support the following types of IDS attack detection:

- DDoS attack detection
- Flooding attack detection
- Spoofing attack detection
- Weak IV detection
- CMCC DoS attack detection

Working Principle

DDoS Attack Detection

DDoS attack means that the attackers send a large number of attack packets toward targeted devices in a short period of time (ARP packets, ICMP packets and SYN packets identified currently) so as to affect legal STAs being associated with the attacked device.

DDoS detection function performs statistics for the attacker's packets and determines whether the number of packets per second exceeds the configured threshold. If yes, this result will be logged. If the dynamic blacklist function is enabled, the attacker will be added into the dynamic blacklist.

Flooding Attack Detection

Flooding attack refers to that an attacker sends a large number of packets of the same type in a short period of time, causing the WLAN devices fail to process legal STA requests due to the Rogue flooding.

Flooding attack detection prevents this flooding attack by continuously monitoring the traffic of each device. Within specified time, when the traffic exceeds the upper limit set by the network administrator, this device is deemed to be a flooding attacker and is therefore blocked. Flooding attack detection can be used with the dynamic blacklist function. When attacks are detected, if the dynamic blacklist function is enabled, the STA initiating the attacks will be added into the dynamic blacklist, ensuring no more intrusion by this STA and thus guaranteeing network security.

Spoofing Attack Detection

Spoofing attack refers to that an attacker sends fake packets in the name of another STA. For example, a fake deauthentication packet causes a STA offline.

WIDS performs detection on the broadcast deauthentication and broadcast disassociation packets. When such packet is received, it is immediately defined as a spoofing attack and logged.

Weak IV Attack Detection

Weak IV (Weak Initialization Vector) attack refers to the following attack behavior: when the WLAN uses WEP encryption, an attacker intercepts packets with weak initialization vectors, cracks the shared key and finally steals the encrypted information.

When WLAN uses WEP for encryption, an initialization vector (IV) is generated for each packet and, together with the shared key, taken as input to generate a key string. With the key string and plain-text encryption, the cipher text is generated finally. When a WEP packet is sent, the IV used for packet encryption is also taken as a part of the packet header to be sent. If the IV is generated with an insecure

method, for example, repetitive IVs are frequently generated or even the same IV is always generated, the shared key will be exposed easily. If a potential attacker obtains the shared key, it can control network resources and pose a threat to network security.

The IDS prevents this attack by identifying the IV of each WEP packet. When a packet with a weak IV is detected, the IDS immediately determines that this is vulnerability and logs this detected result.

CCMC DoS Attack Detection

The CMCC DoS attack detection refers to that for every STA which is connected or tries to access, if the number of Action, Association, Authentication, Deauthentication, Disassociation, Reassociation, Probe Request or Null data packets is larger than the set threshold, an attack is deemed existing.

2.3.3 User Isolation

Because of the mobility and uncertainty of STAs, STA information privacy appears to be particularly important in some occasions (especially public areas). Therefore, direct STA communication should be restricted. The user isolation technology can avoid insecure access between STAs in WLAN coverage (e.g., via online neighborhood), so as to prevent private information from being stolen by others.

User isolation isolates STAs, and prevents them from accessing each other without affecting their normal network access, guaranteeing service security. The layer-2 user isolation has the following five types:

- AP-based user isolation
- AP-SSID based user isolation
- CMCC user isolation

Working Principle

AP-Based User Isolation

Direct communication cannot be conducted between layer-2 STAs associated with the same AP.

AP-SSID based User Isolation

Direct communication cannot be conducted between STAs in the same WLAN who are associated with the same AP.

CMCC User Isolation

CMCC user isolation depends on SSID-based isolation functions. It takes effect on the APs in local forwarding mode.

2.3.4 Rogue Detection and Containment

Network devices are usually divided into two types: illegal (Rogue) and legal. Rogue devices have potential vulnerabilities to be attacked or manipulated, which therefore poses a serious threat or hazard to network security. Rogue detection function can monitor abnormal devices in the whole WLAN, helping the network administrator find hidden dangers in networks.

Rogue detection is applicable to multiple Rogue devices in WLAN: APs, clients, wireless bridges, and Ad-hoc devices. Currently, only the detection on Rogue APs and Ad-hoc devices and unknown STAs is supported.

Rogue device containment counters Rogue devices by sending fake deauthentication frames to the addresses of Rogue devices, as so to prevent STAs from accessing illegal service or illegal STAs from accessing the devices.

Working Principle

Rogue Detection

The Rogue detection function is conducted by an AP in Monitor mode or Hybrid mode. WIDS captures wireless packets in the air by deploying some APs in WLAN and setting them to operate in Monitor or Hybrid mode. By conducting analysis and statistics of monitored wireless packets, the AP can obtain information on the Rogue device. Meanwhile, the network administrator can also prepare illegal device detection rules to monitor abnormal devices in the whole WLAN.

Unknown STA Detection

The unknown STA detection function monitors the probe request packets from non-accessed STAs in the network, and the network administrator can also use configuration to specify information on the unknown STA.

Rogue Containment

The Rogue containment refers to a service which uses the means of simulating fake broadcast deauthentication packets to contain Rogue devices that meet the containment mode rules, and to prevent normal STAs from accessing Rogue devices.

Unknown STA Containment

The unknown STA containment refers to denying unknown STA access by directly constructing deauthentication packets.

CMCC Rogue Detection

The function of CMCC Rogue detection is aimed at preventing illegal APs from interfering with legal APs in signal transmission, and even preventing legal STAs from being cheated out of registration information. Based on Rogue detection function, CMCC Rogue detection cuts off the network connection of illegal APs in collaboration with the background system, if conditions permit.

2.4 Configuration

Configuration	Description and Command	
Configuring Frame Filtering	(Optional) It is used to configure frame filtering.	
	kickout threshold	Configures the low-rate kickout threshold.
	whitelist mac-address	Adds an entry to the whitelist.
	whitelist max	Configures the length of the whitelist.
	static-blacklist mac-address	Adds an entry to the static blacklist.
	static-blacklist max	Configures the length of the static blacklist.
	dynamic-blacklist enable	Enables the dynamic blacklist function.
	dynamic-blacklist lifetime	Configures the lifetime of the dynamic blacklist.
	dynamic-blacklist ac-max	Configures the length of the dynamic blacklist on ACs.
	dynamic-blacklist ap-max	Configures the length of the dynamic blacklist on APs.
	dynamic-blacklist mac-address	Adds an entry to the dynamic blacklist.
	ssid-filter max	Configures the SSID-based blacklist and whitelist and their length.
	ssid-filter blacklist mac-address	Adds an entry to the SSID-based blacklist.
	ssid-filter blacklist max	Configures the length of the SSID-based blacklist, 256 by default.

Configuration	Description and Command	
	ssid-filter whitelist mac-address	Adds an entry to the SSID-based whitelist.
	ssid-filter whitelist max	Configures the length of the SSID-based whitelist, 256 by default.
Configuring IDS	(Mandatory) It is used to configure IDS.	
	attack-detection enable	Specifies the IDS type.
	attack-detection ddos	Configures the interval and packet threshold of DDoS attack detection.
	attack-detection flood multi-mac	Configures the interval and packet threshold of multi-STA flooding attack detection.
	attack-detection flood single-mac	Configures the interval and packet threshold of single-user flood attack detection.
	attack-detection spoof	Configures the interval and packet threshold of the spoofing attack detection.
	attack-detection weak-iv	Configures the interval and packet threshold of the weak IV attack detection.
	attack-detection statistics ac-max	Configures the length of IDS statistics on ACs.
	attack-detection statistics ap-max	Configures the length of IDS statistics on APs.
	dos-detection	Configures CMCC DoS attack detection.
Configuring User Isolation	(Optional) It is used to configure user isolation.	
	user-isolation enable	Enables the AP-based, AP-SSID-based and CMCC layer-2 user isolation.
	user-isolation permit-mac	Adds an entry to the permissible MAC list for user isolation.
	user-isolation permit-mac max	Configures the length of the permissible MAC list for user isolation.
Configuring Rogue Detection and Containment	(Optional) It is used to set the device detection and containment function.	
	countermeasures enable	Enables the Rogue containment function.
	countermeasures ap-max	Configures the maximum number of contained devices once.
	countermeasures channel-match	Enables channel-based containment.
	countermeasures interval	Configures the containment interval.
	countermeasures mode	Configures the containment mode.
	countermeasures rssi-min	Configures the minimum containment RSSI.
	device aging duration	Configures the aging duration of the detected devices.
	device attack mac-address	Adds an entry to the static attack list.
	device attack max	Configures the length of the static attack list.
	device black-ssid	Adds an entry to the SSID-based blacklist.
	device max-black-ssid	Configures the length of the SSID-based blacklist.

Configuration	Description and Command	
	device friendly-flags	Configures the device friendly flag.
	device permit mac-address	Adds an entry to the permissible MAC list.
	device permit mac-address max	Configures the length of the permissible MAC list.
	device permit ssid	Adds an entry to the permissible SSID list.
	device permit max-ssid	Configures the length of the permissible SSID list.
	device permit vendor bssid	Adds an entry to the permissible vendor list.
	device permit vendor bssid max	Configures the length of the permissible vendor list.
	device unknown-sta dynamic-enable	Enables unknown STA detection and containment.
	device unknown-sta mac-address	Adds an entry to the unknown STA list
	device unknown-sta mac-address max	Configures the length of the unknown STA list.
	device channel-bind radio	Configures the scanning channel of a specified radio.
	device scan-para	Configures the CMCC illegal AP detection.
	device detected-ap-max	Configures the maximum number of detected APs.
	hybrid-scan radio	Configures the scanning status of a specified radio.
	scan-channels { 802.11a | 802.11b } channels	Configures the scanning channel of a specified AP.
	rogue-ap countermeasures enable	Enables CMCC Rogue containment.
configuring AP Working Modes	(Optional) It is used to set the AP working mode.	
	device mode	Configures the AP working mode.

2.4.1 Configuring Frame Filtering

Configuration Effect

- Configure the frame filtering rules to provide packet filtering services.

Notes

- An STA cannot be configured in both the static blacklist and the whitelist.
- An STA cannot exist in both the blacklist and whitelist of the same SSID.

Configuration Steps

Configuring the Low-Rate Filter

- (Optional) The **kickout threshold** command is used in WIDS configuration mode to configure the low-rate kickout threshold. The low-rate filtering function effectively works only after the low-rate kickout threshold is configured (larger than 0).
- Unless otherwise noted, enable this function only on ACs which needs to support the low-rate STA filtering function.

Command	**kickout threshold** *rate*
Parameter Description	*rate*: Indicates the low-rate kickout threshold ranging from 0 to 130 Mbps.

Defaults	By default, low-rate STAs are not filtered out, and the kickout threshold is 0.
Command Mode	WIDS configuration mode
Usage Guide	The STAs can select different low-rate STA filtering thresholds based on requirements.

Configuring the Whitelist

- Optional.
- Unless otherwise noted, enable this function only on ACs which need the whitelist function.
- To configure the whitelist entry, the same as above.
- To configure the whitelist length, the same as above.
- Run the **whitelist mac-address** command to add an entry to the whitelist in WIDS configuration mode. The whitelist filtering function effectively works only after an effective whitelist entry is configured.
- Run the **whitelist max** command to configure the maximum number of entries in the whitelist in WIDS configuration mode.

Command	**whitelist** { **mac-address** *H.H.H* | **max** *num* }
Parameter Description	**mac-address** *H.H.H*: Indicates the MAC address of a whitelist entry. **max** *num*: Indicates the length of the whitelist ranging from 1 to 2,048.
Defaults	By default, the whitelist is empty and the whitelist length is 1,024.
Command Mode	WIDS configuration mode
Usage Guide	The whitelist function takes effect only when the whitelist has entries.

Configuring the Static Blacklist

- Optional.
- Unless otherwise noted, enable this function only on ACs which need the static blacklist function.
- To configure the static blacklist entry, the same as above.
- To configure the static blacklist length, the same as above.
- Run the **static-blacklist mac-address** command to add an entry to the static blacklist in WIDS configuration mode. The static blacklist filtering function effectively works only after an effective static blacklist entry is configured.
- Run the **static-blacklist max** command to configure the maximum number of entries in the static list in WIDS configuration mode, indicating the maximum number of permissible static blacklist entries on the device.

Command	**static-blacklist** { **mac-address** *H.H.H* | **max** *num* }
Parameter Description	**mac-address** *H.H.H*: Indicates the MAC address of a static blacklist entry. **max** *num*: Indicates the length of the static blacklist ranging from 1 to 2,048.
Defaults	By default, the static blacklist is empty and the static blacklist length is 1,024.
Command Mode	WIDS configuration mode
Usage Guide	The static blacklist function takes effect only when the static blacklist has entries.

Configuring the Dynamic Blacklist

- Optional.
- Unless otherwise noted, enable this function only on ACs which need the dynamic blacklist function.
- Run the **dynamic-blacklist enable** command to enable the dynamic blacklist function in WIDS configuration mode. A dynamic blacklist entry is generated dynamically along with the IDS attack detection and works only after the dynamic blacklist function is enabled.
- Run the **dynamic-blacklist lifetime** command to configure the service life of the dynamic blacklist in WIDS configuration mode, indicating how long the dynamic blacklist exists in the device.
- Run the **dynamic-blacklist** { **ac-max** | **ap-max** } command to configure the maximum number of dynamic blacklist entries on both ACs and APs in WIDS configuration mode.
- Run the **dynamic-blacklist mac-address** command to add an entry to the dynamic blacklist in WIDS configuration mode.

Command	**dynamic-blacklist** { **enable** | **lifetime** *time* |**ac-max** *num* |**ap-max** *num* /**mac-address** *H.H.H* }
Parameter Description	**enable**: Enables the dynamic blacklist function **lifetime** *time*: Indicates the service life of the dynamic blacklist ranging from 60 to 86,400 seconds. **ac-max** *num*: Indicates the length of the dynamic blacklist on ACs. **ap-max** *num*: Indicates the length of the dynamic blacklist on APs. **mac-address** *H.H.H*: Indicates the MAC address of a dynamic blacklist entry.
Defaults	By default, the dynamic blacklist function is disabled. The default length of the dynamic blacklist is 2,048 on ACs and APs with 300-second lifetime.
Command Mode	WIDS configuration mode
Usage Guide	A dynamic blacklist entry is generated in the IDS attack detection function.

Configuring the SSID-Based Blacklist

- Optional.
- Unless otherwise noted, enable this function only on ACs which need the SSID-based blacklist function.
- To configure the SSID-based blacklist entry, the same as above.
- To configure the SSID-based blacklist length, the same as above.
- To configure the SSID list length, the same as above.
- Run the **ssid-blacklist mac-address** command to add an entry to the SSID-based static blacklist in WIDS configuration mode. The static blacklist filtering function effectively works only after an effective static blacklist entry is configured.
- Run the **ssid-filter blacklist max** command to configure the maximum number of entries in the SSID-based static blacklist in WIDS configuration mode.
-

Command	**ssid-filter** { **max** *num* | **blacklist mac-address** *H.H.H* **in-ssid** *string* | **blacklist max** *num* }
Parameter Description	**max** *num*: Indicates the maximum length of the SSID-based blacklist, ranging from 1 to 128. The default is 64. **blacklist mac-address** *H.H.H* **in-ssid** *string*: Adds an entry to the specified SSID-based blacklist. **blacklist max** *num*: Configures the length of the SSID-based blacklist, ranging from 1 to 256.
Defaults	The SSID-based blacklist is empty.

Command Mode	WIDS configuration mode
Usage Guide	This function takes effect only when the SSID-based blacklist has entries.

Configuring the SSID-Based Whitelist

- Optional.
- Unless otherwise noted, enable this function only on ACs which need the SSID-based whitelist function.
- To configure the SSID-based whitelist entry, the same as above.
- To configure the SSID-based whitelist length, the same as above.
- Run the **ssid-filter whitelist mac-address** command to add an entry to the SSID-based whitelist in WIDS configuration mode. The whitelist filtering function effectively works only after an effective whitelist entry is configured.
- Run the **ssid-filter whitelist max** command to configure the maximum number of entries in the SSID-based whitelist in WIDS configuration mode.

Command	**ssid-filter** { **whitelist mac-address** *H.H.H* **in-ssid** *string* | **whitelist max** *num* }
Parameter Description	**whitelist mac-address** *H.H.H* **in-ssid** *string*: Configures the whitelist entry for a specified SSID. **whitelist max** *num*: Configures the length of the SSID-based whitelist, ranging from 1 to 256.
Defaults	The SSID-based whitelist is empty.
Command Mode	WIDS configuration mode
Usage Guide	This function takes effect only when the SSID-based whitelist has entries.

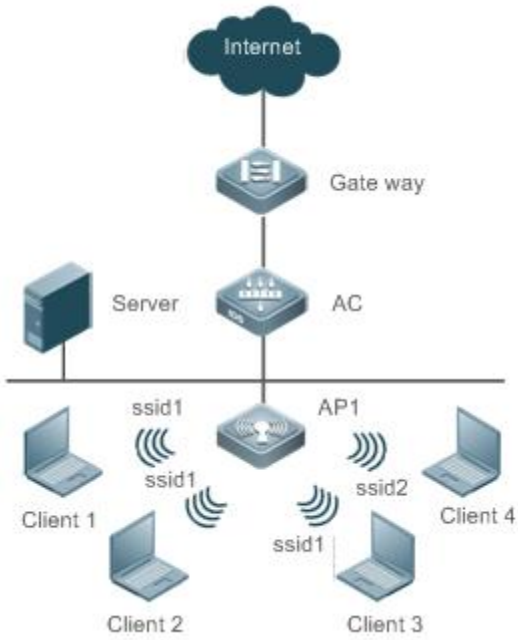
Verification

Conduct related function verifications based on corresponding frame filtering rules.

- Check the low-rate STA filtering function. The packets are discarded and the low-rate STAs are successfully removed.
- Check the whitelist function. When the whitelist is configured, the STAs not included in the whitelist cannot join the AP.
- Check the static blacklist function. When the static blacklist is configured, the STAs included in the static blacklist cannot join the AP.
- Check the dynamic blacklist function. When the dynamic blacklist function is enabled, entries in the dynamic blacklist can be generated along with the IDS attack detection, and STAs in the dynamic blacklist cannot join the AP again.
- Check the SSID-based blacklist function. When the SSID-based blacklist is configured, STAs in the SSID-based blacklist cannot join this SSID service.
- Check the SSID-based whitelist function. When the SSID-based whitelist is configured, STAs not included in the SSID-based whitelist cannot join this SSID service.

Configuration Example

Configuring the Whitelist Entry

Scenario Figure 2- 5	
Configuration Steps	● Add an entry to thewhitelist on the AC.
	FS# configure terminal FS(config)# wids FS(config-wids)# whitelist mac-address 0000.0000.0001
Verification	After the STA configures the whitelist entry, the following methods can be used to check the configuration. ● Run the **show wids whitelist** command to display the information on related parameters configured onthe STA. ● Use the device to verify whether the function has taken effect.
	FS#show wids whitelist ---------- Whitelist Information ---------- num Mac-address 1 0000.0000.0001

Common Errors

N/A

2.4.2 Configuring IDS

Configuration Effect

- IDS can be used to timely find and defend against malicious or unintentional attacks in WLAN.

Notes

- IDS needs to be used together with the dynamic blacklist function, to effectively prevent attacks against WLAN.

Configuration Steps

Specifying the IDS Type

- (Optional) IDS is disabled by default.
- Unless otherwise noted, configure this function on ACs which need the IDS attack detection function.
- To configure the IDS attack detection, the same as above.

Command	**attack-detection enable** { **all** | **ddos** | **flood** | **spoof** | **weak-iv** }
Parameter Description	**ddos**: Enables DDoS attack detection. **flood**: Enables flooding attack detection. **spoof**: Enables spoofing attack detection. **weak-iv**: Enables Weak IV attack detection. **all**: Enables all IDS attack detection.
Defaults	All IDS attack detection is disabled by default.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring DDoS Attack Detection

- Optional.
- Unless otherwise noted, configure this function on ACs which need DDoS attack detection.
- To configure the thresholds and intervals of a specified type of packets in DDoS attack detection, the same as above.

Command	**attack-detection ddos** { **arp-threshold** *num*| **icmp-threshold** *num*| **syn-threshold** *num* | **interval** *time* }
Parameter Description	**arp-threshold** *num*: Indicates ARP packet threshold ranging from1 to 10,000 pps. **icmp-threshold** *num*: Indicates ICMP packet threshold ranging from110,000 pps. **syn-threshold** *num*: Indicates SYN packet threshold ranging from1 to 10,000 pps. **interval** *time*: Indicates the period of DDoS attack detection ranging from 10 to 60 seconds.
Defaults	By default, the interval of DDoS attack detection is 30 seconds, and the three DDoS attack detection thresholds are 5 pps for ARPpackets, 100 pps for ICMPpackets, and 5 pps for SYN packets.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring Flooding Attack Detection

- (Optional) Flooding attack detection is disabled by default.
- Unless otherwise noted, configure this function on ACs which need the flooding attack detection.
- To configure the threshold and interval of a specified types of packets in flooding attack detection, the same as above.
- Run the **attack-detection flood single-mac** { **total** \| **assoc** \| **reassoc** \| **disassoc** \| **probe** \| **action** \| **auth** \| **deauth** \| **null-data** } **threshold***num***interval***time* command to configure the threshold and interval of a specified type of packets for single-STAflooding attack in WIDS configuration mode.

- Run the **attack-detection flood multi-mac** { **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** } **threshold** *num* **interval** *time* command to configure the threshold and interval of a specified type of packets for multi-STA flooding attack in WIDS configuration mode.

Command	**attack-detection flood single-mac** { **total** | **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** } **threshold** *num* **interval** *time*
Parameter Description	**single-mac**: Indicates single STA detection. **total**: Indicates all packets. **assoc**: Indicates Association packets. **reassoc**: Indicates Reassociation packets. **disassoc**: Indicates Disassociation packets. **probe**: Indicates Probe packets. **action**: Indicates Action packets. **auth**: Indicates Authentication packets. **deauth**: Indicates Deauthentication packets. **null-data**: Indicates Null packets. *num*: Indicates the packet threshold of flooding attack detection ranging from 1 to 5,000. *time*: Indicates the interval of flooding attack detection ranging from 10 to 60 seconds.
Defaults	All packet thresholds of flooding attack detection, by default, 300 for single-STA, 500 for multi-STA, and 10 seconds of the statistic interval
Command Mode	WIDS configuration mode
Usage Guide	N/A

Command	**attack-detection flood multi-mac** { **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** } **threshold** *num* **interval** *time*
Parameter Description	**multi-mac**: Indicates multi-STA detection. **assoc**: Indicates Association packets. **reassoc**: Indicates Reassociation packets. **disassoc**: Indicates Disassociation packets. **probe**: Indicates Probe packets. **action**: Indicates Action packets. **auth**: Indicates Authentication packets. **deauth**: Indicates Deauthentication packets. **null-data**: Indicates Null packets. *num*: Indicates the packet threshold of flooding attack detection ranging from 1 to 5,000. *time*: Indicates the interval of flooding attack detection ranging from 10 to 60 seconds.
Defaults	All packet thresholds of flooding attack detection, by default, 300 for single-STA, 500 for multi-STA, and 10 seconds of the statistic interval
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring Spoofing Attack Detection

- (Optional) Spoofing attack detection is disabled by default.
- Unless otherwise noted, configure this function on ACs which need the spoofing attack detection.
- To configure the threshold and interval of a specified type of packets in spoofing attack detection, the same as above.

Command	**attack-detection spoof** { **threshold** *num* |**interval** *time* }
Parameter Description	**threshold** *num*: Indicates the packet threshold of spoofing attack detection ranging from 1 to 1,000. **interval** *time*: Indicates the interval of spoofing attack detection ranging from 10 to 60 seconds.
Defaults	By default, the packet threshold is 1 and the detection interval is 50 seconds.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring Weak IV Attack Detection

- (Optional) The Weak IV attack detection function is disabled by default.
- Unless otherwise noted, configure this function on ACs which needs the Weak IV attack detection.
- To configure the thresholds and intervals for specified types of packets in Weak IV attack detection, the same as above.

Command	**attack-detection weak-iv** { **threshold** *num*| **interval** *time* }
Parameter Description	**threshold** *num*: Indicates the packet threshold of weak IV attack detection ranging from 1 to 10,000. **interval** *time*: Indicates the interval of weak IV attack detection ranging from 1 to 60 seconds.
Defaults	The default interval of Weak IV detection is 15 seconds, and the default detection threshold is 10.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring CMCC DoS Attack Detection

- (Optional) CMCC DoS attack detection is disabled by default.
- Unless otherwise noted, configure this function on ACs which need the Weak IV attack detection.
- To configure the threshold and interval of a specified type of packets in CMCC DoS attack detection, the same as above.

Command	**dos-detection** { **enable** | **threshold** *num*| **interval** *time* }
Parameter Description	**enable:** Enables CMCC DoS attack detection **threshold** *num*: Indicates the packet threshold of CMCC DoS attack detection ranging from 1 to 5,000. **interval** *time*: Indicates the interval of the CMCC DoS attack detection ranging from 1,000 to 60,000 ms.
Defaults	The interval of CMCC DoS attack detection is 1,000 ms, and the detection threshold is 30.
Command Mode	WIDS configuration mode
Usage Guide	N/A

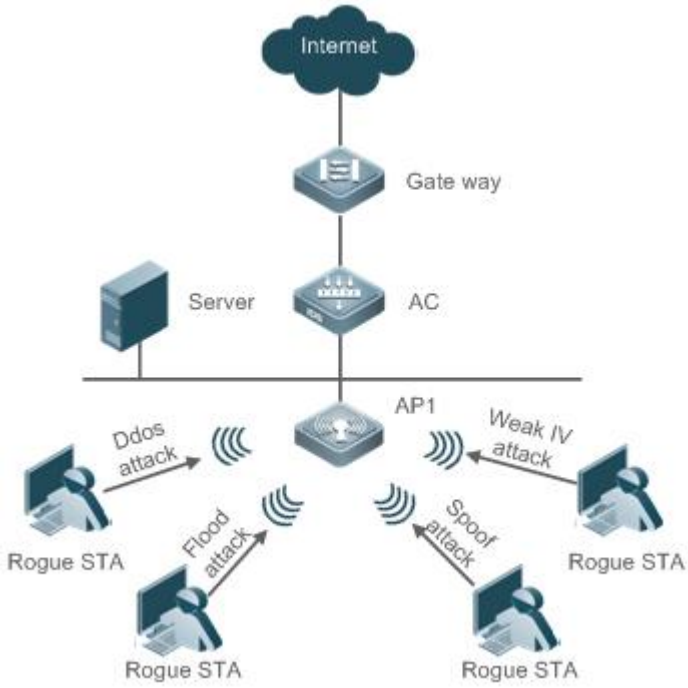
Verification

Carry out related verifications based on the IDS attack detection type:

- DDoS attack detection, detecting the ARP packet attack, ICMP packet attack and SYN packet attack.
- Flooding attack detection, detecting the multi-STA flooding attack and single-STA flooding attack.
- Spoofing attack detection, detecting the broadcast disassociation and deauthentication packet attacks.
- Weak IV attack detection, detecting the weak IV packet attack.
- CMCC DoS attack detection, detecting the DoS attack.

Configuration Example

Configuring DDoS Attack Detection

Scenario **Figure 2- 6**	
Configuration Steps	● Specify the IDS type and configure related thresholds on the AC.
	FS# configure terminal FS(config)# wids FS(config-wids)# attack-detection enable flood FS(config-wids)# attack-detection ddos interval 10
Verification	● If a DDoS attack exists, related syslog information will be printed on the AC.
	*Feb 7 13:37:03: %WIDS-6-ATTACK: Client(0025.64b8.2ffa): ARP DDOS attack to Ap (1414.0902.0016). Feb 7 13:37:03: %WIDS-6-ATTACK: Client(0025.64b8.2ffa): ICMP DDOS attack to Ap (1414.0902.0016). Feb 7 13:37:03: %WIDS-6-ATTACK: Client(0025.64b8.2ffa): SYN DDOS attack to Ap (1414.0902.0016).

Common Errors

N/A

2.4.3 Configuring User Isolation

Configuration Effect

- After user isolation is configured, direct communication cannot be conducted between STAs meeting the user isolation rules.

Notes

- User isolation is only valid for layer-2STAs.

Configuration Steps

Configuring the User Isolation Mode

- Optional.
- Unless otherwise noted, configure this function on ACs.

Command	**user-isolation** { **ap** | **ssid-ap** | **wlan-id** *num* } **enable**
Parameter Description	**ap:** Indicates AP-based layer-2 user isolation. **ssid-ap:** Indicates AP-SSID-based layer-2 user isolation. **wlan-id** *num*: Indicates SSID-based layer-2 user isolation.
Defaults	User isolation is disabled.
Command Mode	WIDS configuration mode
Usage Guide	The AC-based and AC-SSID-based layer-2 user isolation are effective only in centralized forwarding mode.

Configuring the Permissible MAC List for User Isolation

- Optional.
- Unless otherwise noted, configure this information on ACs.
- To configure the isolation list length, the same as above.

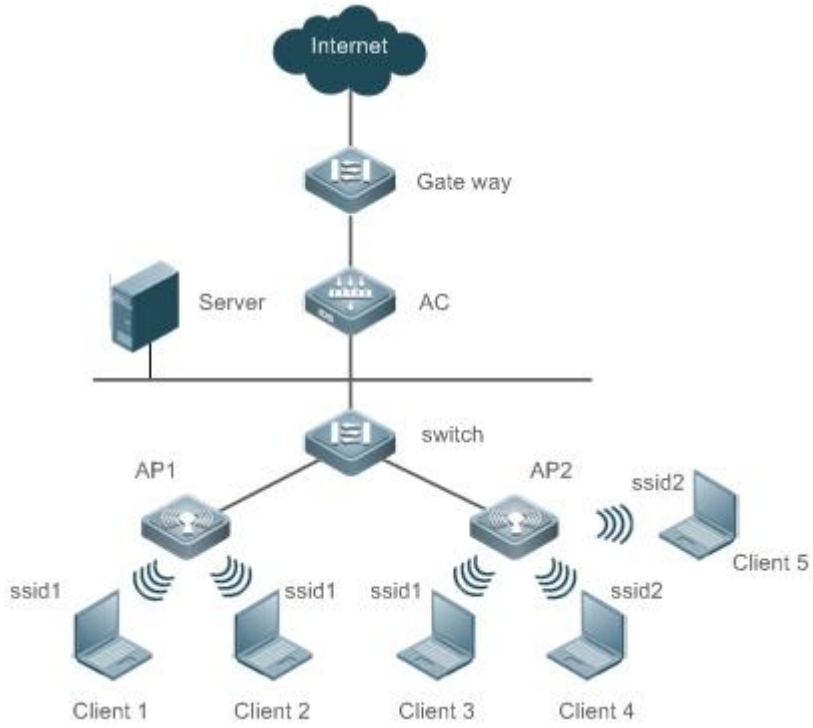
Command	**user-isolation permit-mac** {*H.H.H* / **max** *num* }
Parameter Description	*H.H.H*: Indicates the permissible MAC list entry for user isolation. **max** *num*: Indicates the permissible MAC list length for user isolation ranging from 1 to 1,024.
Defaults	The permissible STA's MAC list for isolation is empty, with the default length of 1,024.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Verification

- Carry out related verifications based on the isolation mode.

Configuration Example

Configuring User Isolation

Scenario	
Figure 1- 7	
Configuration Steps	● Configure the AP-based layer-2 user isolation on the AC.
	FS# configure terminal FS(config)# wids FS(config-wids)# user-isolation ap enable
Verification	● Run the **show running-config** command to display the information on related parameters configured by the STA.
	FS#show running-config … ! wids user-isolation ap enable !

Common Errors

N/A

2.4.4 Configuring Rogue Detection and Containment

Configuration Effect

Configure Rogue detection and containment provide illegal device suppression and maintain WLAN security.

Notes

The detection and containment of Rogue devices takes effect only when the AP working mode is Hybrid or Monitor.

Configuration Steps

Enabling Rogue Containment

- Optional. Run the **countermeasures enable** command to enable Rogue containment in WIDS configuration mode.
- Unless otherwise noted, this function is configured on ACs which need the Rogue containment function.

Command	**countermeasures enable**
Parameter Description	N/A
Defaults	Rogue containment is disabled.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Containment Interval

- Optional. Run the **countermeasures interval** *time* command to configure the interval of Rogue containment in WIDS configuration mode.
- Unless otherwise noted, configure the containment interval on ACs which need the Rogue device containment period.

Command	**countermeasures interval** *time*
Parameter Description	time: Indicates the containment interval ranging from 100 to 10,000 ms.
Defaults	The default containment interval is 1,000 ms.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Containment Mode

- Optional. Run the **countermeasures mode** { **all** | **adhoc** | **config** | **rogue** | **ssid** } command to configure the Rogue containment mode in WIDS configuration mode.
- Unless otherwise noted, configure this on ACs which need Rogue containment mode.

Command	**countermeasures mode** { **all** | **adhoc** | **config** | **rogue** | **ssid** }
Parameter Description	**adhoc**: Indicates Ad-hoc containment mode, countering Ad-hoc devices. **config**: Indicates Config containment mode, countering devices which meet entries in the SSID blacklist and static attack list. **rogue**: Indicates Rogue containment mode, countering devices whose RSSI is larger than the threshold. **ssid**: Indicates SSID containment mode, countering devices with the same SSID but not on the same AC. **all**: Indicates all the above containment modes.

Defaults	No containment mode is specified by default.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Static Attack List

- Optional. Run the **device attack mac-address** *H.H.H* command to configure the static attack statistic list information in WIDS configuration mode.
- Unless otherwise noted, configure this on ACs which need the static attack list.

Command	**device attack** { **mac-address** *H.H.H* | **max** *num* }
Parameter Description	**mac-address** *H.H.H*: Indicates the MAC address of a static attack list entry. **max** *num*: Indicates the length of the static attack list, ranging from 1 to 1,024.
Defaults	The static attack list is empty, and the length of the static attack list is 512 by default.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the SSID-based Blacklist

- Optional. Run the **device black-ssid** *ssid* command to configure the SSID blacklist information in WIDS configuration mode.
- Unless otherwise noted, configure this on ACs which need the SSID blacklist.

Command	**device** { **black-ssid** *ssid* | **max-black-ssid** *num* }
Parameter Description	**black-ssid** ssid: Indicates the SSID blacklist entry. **max-black-ssid** *num*: Indicates the SSID blacklist length, ranging from 1 to 1,024.
Defaults	The SSID blacklist is empty, and the SSID blacklist length is 512 by default.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Lists of Permissible MACs, SSIDs and Vendors

- Optional.
- Unless otherwise noted, configure these on ACs which need the permissible MAC, permissible SSID and permissible vendor lists.
- Run the **device permit mac-address** *H.H.H* command to configure the permissible MAC list entry in WIDS configuration mode.
- Run the **device permit ssid** *H.H.H* command to configure the permissible SSID list entry in WIDS configuration mode.
- Run the **device permit vendor** *H.H.H* command to configure the permissible vendor list entry in WIDS configuration mode.

Command	**device permit** { **mac-address** *H.H.H* | **mac-address max** *num* | **ssid** *ssid* | **max-ssid** *num* | **vendor bssid** *H.H.H* | **vendor bssid max** *num* }
Parameter Description	**mac-address** *H.H.H*: Indicates the permissible MAC list entry, null by default. **mac-address max** *num*: Indicates the permissible MAC list length, ranging from 1 to 2,048, 1,024 by default.

	ssid *ssid*: Indicates the permissible SSID list entry, null by default. **max-ssid** *num*: Indicates the permissible SSID list length, ranging from 1 to 1,024, 512 by default. **vendor bssid** *H.H.H*: Indicates the permissible vendor list entry, null by default. **vendor bssid max** *num*: Indicates the permissible vendor list length, ranging from 1 to 1,024, 512 by default.
Defaults	See the **Parameter Description**.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Maximum Number of Contained Devices Once

- Optional. Run the **countermeasures ap-max** *ap-num* command to configure the quantity of one-time Rogue device containment in WIDS configuration mode.
- Unless otherwise noted, configure this on ACs which need to configure the contained Rogue device quantity.

Command	**countermeasures ap-max** *ap-num*
Parameter Description	*ap-num*: Indicates the maximum number of countered devices each time, ranging from 1 to 256.
Defaults	The default maximum number of countered devices is 30.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Aging Duration of the Detected Devices

- Optional. Run the **device aging duration** *time* command to configure the aging duration of the detected devices in WIDS configuration mode.
- Unless otherwise noted, configure this on ACs which need the aging time.

Command	**device aging duration** *time*
Parameter Description	*time*: Indicates the aging duration, ranging from 500 to 5,000 seconds.
Defaults	The default aging duration is 1,200 seconds.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Device Friendly Flag

- Optional. Run the **device friendly-flags** *value* command to configure the device friendly flag in WIDS configuration mode. With the device friendly flag, the AP device can identify devices on the same AC.
- Unless otherwise noted, configure this on ACs which need the device friendly flag.

Command	**device friendly-flags** *value*
Parameter	*value*: Indicates the device friendly flag, ranging from 1 to 4294967295.

Description	
Defaults	The default value is 0.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Minimum Containment RSSI

- Optional. Run the **countermeasures rssi-min** *num* command to configure the minimum containment RSSI in WIDS configuration mode. A Rogue device which exceeds this RSSI will be countered.
- Unless otherwise noted, configure this on ACs which need logs to be written into the memory buffer.

Command	**countermeasures rssi-min** *num*
Parameter Description	*num*: Indicates the minimum containment RSSI, ranging from 0 to 75 (-95 to -20).
Defaults	The default minimum containment RSSI is 25 (-70) by default.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Enabling Channel-Based Containment

- Optional. Run the **countermeasures channel-match** command to enable channel-based containment function in WIDS configuration mode. The channel-based containment can be conducted based on the channel on which the detected Rough device operates.
- Unless otherwise noted, configure this on ACs which need the channel-based containment function.

Command	**countermeasures channel-match**
Parameter Description	**channel-match**: Enables channel-based containment.
Defaults	Channel-based containment is disabled.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Enabling Unknown STA Detection and Containment

- Optional.
- Unless otherwise noted, configure this on ACs which need the unknown STA detection and containment function.
- Run the **device unknown-sta dynamic-enable** command to enable the unknown STA detection and containment function in WIDS configuration mode.
- Run the **device unknown-sta mac-address** *H.H.H* command to configure the unknown STA list entry in WIDS configuration mode.

Command	**device unknown-sta** { **dynamic-enable** | **mac-address** *H.H.H* | **mac-address max** *num* }
Parameter	**dynamic-enable**: Enables unknown STA detection and containment.

Description	**mac-address** *H.H.H*: Configures the unknown STA list entry, empty by default. **mac-address max** *num*: Configures the unknown STA list length, ranging from 1 to 256.
Defaults	Unknown STA detection and containment is disabled.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring CMCC Rogue Detection

- Optional.
- Unless otherwise noted, configure these on ACs which need the function of CMCC Rogue detection.
- Run the **device channel-bind radio** *radio-id* { **channel** *num*| **max-cycles** *value* } command to configure the scanning channel of a specified radio for CMCC Rogue detection in AP configuration mode.
- Run the **device scan-para** { **radio** *radio-id* **scan-type** { **active** | **passive** } **device-detect** { **enable** | **disable** } | **ap-mode** { **normal** | **monitor** } | **detect-rpt-time** *time* } command to configure the scanning parameters for detection of interoperability with illegal APs in AP configuration mode.
- Run the **rogue-ap countermeasures enable** command to configure the function of containing interoperability with illegal APs in WIDS configuration mode.
- Configure the scanning channel information on interoperability with illegal APs

Command	**device channel-bind radio** *radio-id*{ **channel** *num* | **max-cycles** *value* }
Parameter Description	*radio-id*: Indicates Radio ID of a specified AP. **channel** *num*: Channel value, Chinese channel by default. **max-cycles** *value*: indicates the number of scanning times, 10 by default and ranging from 0 to 255.
Defaults	For details, see the **Parameter Description**.
Command Mode	AP configuration mode
Usage Guide	N/A

Command	**device scan-para** { **radio** *radio-id* **scan-type** { **active** | **passive** } **device-detect** { **enable** | **disable** } | **ap-mode** { **normal** | **monitor** } | **detect-rpt-time** *time* }
Parameter Description	**radio** *radio-id*: Radio ID **scan-type active**: Indicates active scanning. The default scanning is passive scanning. **scan-type passive**: Indicates passive scanning. **device-detect enable**: Enables the detection. The detection is disabled by default. **device-detect disable**: Disables the detection. **ap-mode normal**: Indicates The AP works in Normal mode. **ap-mode monitor**: Indicates The AP works in Monitor mode. **detect-rpt-time** time: Indicates the detection reporting period, 60 seconds by default, ranging from 60 to 120 seconds.
Defaults	For defaults, see the **Parameter Description**.

Command Mode	AP configuration mode
Usage Guide	N/A

Command	**rogue-ap countermeasures enable**
Parameter Description	N/A
Defaults	Disabled.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring the Maximum Number of Detected APs

- Optional. Run the **device detected-ap-max** *num* command to configure the maximum number of detected APs in WIDS configuration mode. A smaller configuration value leads to less data being detected on the AP. If less data is detected, the device containment function may not show an obvious containment effect. A larger configuration value requires more memory.
- Unless otherwise noted, configure this on ACs which need the maximum number of detected APs.

Command	**device detected-ap-max** *num*
Parameter Description	*num*: Indicates the maximum number of detected APs, ranging from 1 to 4,096.
Defaults	The default maximum number is 2,048.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring the Scanning Status of a Specified Radio

- Optional. Run the **hybrid-scan radio** *num* **{ disable | enable }** command to configure the scanning status of a specified radio in AP configuration mode. If disabling the configuration leads to AP working in non-normal mode, there will be no device detection data.
- Unless otherwise noted, configure this on ACs which need the radio scanning status.

Command	**hybrid-scan radio** *num* **{ enable | disable }**
Parameter Description	*num*: Indicates a radio ID.
Defaults	All radio scanning is enabled by default.
Command Mode	AP configuration mode
Usage Guide	N/A

Configuring the Scanning Channel of a Specified AP

- Optional. Run the **scan-channels { 802.11a | 802.11b } channels** *num1 num2…num13* command to configure the scanning channel in AP configuration mode. If the scanning channel is not configured, there will be no device detection data when the AP operates not in Normal mode.
- Unless otherwise noted, configure this on ACs which need the specified AP scanning channel.

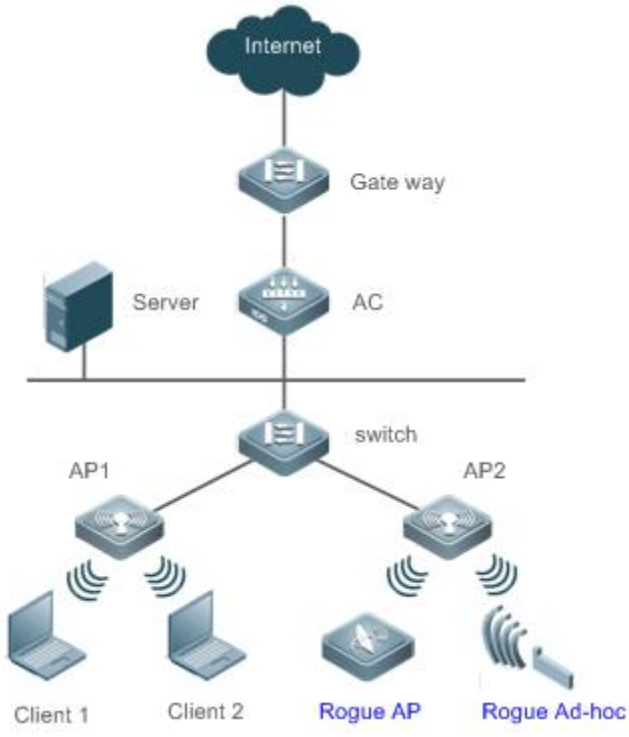
Command	**scan-channels { 802.11a | 802.11b } channels** *num1 num2…num13*
Parameter Description	*num*: Indicates a channel number.
Defaults	The scanning channel is null.
Command Mode	AP configuration mode
Usage Guide	N/A

Verification

- Run the **show wids detected** command to display the detected results.

Configuration Example

Configuring Rogue Containment

Scenario	
Figure 2-8	
Configuration Steps	• Configure Rogue containment information on the AC. Before configuring containment, confirm that the WLAN service has been deployed on the contained AP; otherwise, the containment will not take effect.
	If the containing AP has joined the default group, view whether the default group has been bound with wlan on the AC.

	FS#show ap-group intf-wlan-map default If the default group is not bound with the wlan service, the wlan service needs to be configured. FS# configure terminal FS(config)# wlan-config 15 wids-monitor FS(config-wlan)# no enable-broad-ssid FS(config-wlan)# ap-group default FS(config-group)#interface-mapping 15 1 The containment takes effect only after the wlan service is configured and the wids function is enabled: FS# configure terminal FS(config)# wids FS(config-wids)# countermeasures enable FS(config-wids)# countermeasures mode ssid
Verification	● Run the **show running-config** command to display the information on related parameters configured by the STA and the log information generated by the system recently.
	FS#show running-config FS#show running-config … ! wids countermeasures enable countermeasures mode SSID ! …

Common Errors

N/A

2.4.5 Configuring AP Working Mode

Configuration Effect

- Based on the configured working mode, the AP can provide different services.

Notes

N/A

Configuration Steps

Configuring AP Working Modes

- Optional.
- Unless otherwise noted, configure this on each AP.

Command	**device mode** { **hybrid** | **monitor** | **normal** }

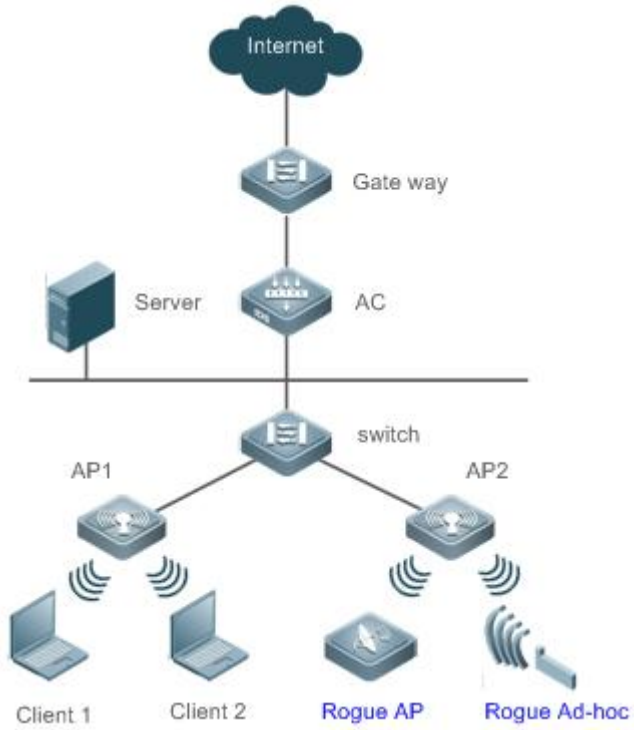
Parameter Description	**hybrid**: Indicates Hybrid mode, in which the device provides both monitoring service and access service. **monitor:** Indicates Monitor mode, in which the device provides only the monitoring service. **normal**: Indicates Normal mode, in which the device provides only the access service.
Defaults	The working mode of the AP is Normal.
Command Mode	AP configuration mode
Usage Guide	N/A

Verification

- Run the **show ap-config running** *ap-name* command to display the current working mode of the AP.

Configuration Example

Configuring the AP Working Mode

Scenario **Figure 2- 9**	
Configuration Steps	● Configure the working mode of a specified AP on the AC.
	FS# configure terminal FS(config)# ap-config ap220 FS (config-ap)#device mode hybrid
Verification	● Run the **show ap-config running** *ap-name* command to display the information on related parameters configured by the STA.
	FS#show ap-config running ap220

```
!
ap-config ap220
 device mode hybrid
 11acsupport enable radio 1
 11acsupport enable radio 2
 802.11n mcs support 23 radio 1
 802.11n mcs support 23 radio 2
 802.11ac mcs support 29 radio 1
 802.11ac mcs support 29 radio 2
 antenna receive 7 radio 1
 antenna receive 7 radio 2
 antenna transmit 7 radio 1
 antenna transmit 7 radio 2
!
```

Common Errors

N/A

2.5 Monitoring

Displaying

Description	Command
Displays the attack list configuration.	**show wids attack-list**
Displays the dynamic or static blacklist configuration.	**show wids blacklist** { **dynamic** | **static** }
Displays the SSID-based blacklist configuration.	**show wids black-ssid**
Displays the information of detected devices of a specified type.	**show wids detected** { **adhoc** | **all** | **friendly ap** |**interfering ap** | **rogue** { **adhoc-ap** | **ap** | **client** | **config-ap** | **ssid-ap** } | **mac-address** *H.H.H* }
Displays the SSID-based blacklist and whitelist configuration.	**show wids ssid-filter** { **blacklist all** [**in-ssid** *string*] | **ssid all** | **whitelist all** [**in-ssid string**] }
Displays the configuration of permissible MAC, permissible SSID and permissible vendor lists.	**show wids permitted** { **mac-address** | **ssid** | **vendor** }
Displays the IDS information.	**show wids statistics**
Displays the unknown STA list configuration.	**show wids unknown-sta**
Displays the permissible MAC entries for user isolation.	**show wids user-isolation permit-mac**
Displays the whitelist entries.	**show wids whitelist**
Displays other WIDS configuration.	**show running-config**
Displays the CMCC DoS detection information.	**show wids dos-detected**
Displays the CMCC Rogue detection information.	**show wids rogue-ap detected**

Chapter 15 WLAN Basic Configuration

1. Configuring APMG
2. Configuring STA Management
3. Configuring CAPWAP
4. Configuring WBS
5. Configuring ETH-MNG
6. Configuring DATA-PLANE
7. Configuring WLOG

1 Configuring APMG

1.1 Overview

Tailored for the wireless network structures that support centralized management, AP Management (APMG) implements centralized management and configuration of access points (APs).

A Wireless Local Area Network (WLAN) refers to a network system that allows different PCs to communicate and share resources with each other by interconnecting different PCs through wireless communication technologies. The essence of a WLAN is that PCs are interconnected with each other in wireless rather than wired mode, thus constructing a network and allowing terminals to move more flexibly.

A traditional WLAN adopts the fat AP network structure in which APs work independently. On the traditional WLAN, each AP must be separately configured and managed, which increases the complexity of network management and O&M workload. In addition, problems, such as radio interference between APs and roaming of wireless users, cannot be effectively resolved due to poor collaboration between APs. To address these issues, a wireless network structure that supports centralized management emerges. This network structure consists of access controllers (ACs) and fit APs, and is also called fit AP network structure. In this network structure, APs are connected to ACs through the Control and Provisioning of Wireless Access Points (CAPWAP), and ACs perform centralized management on APs.

Protocols and Standards

- RFC5415: Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification
- RFC5416: Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11

1.2 Application

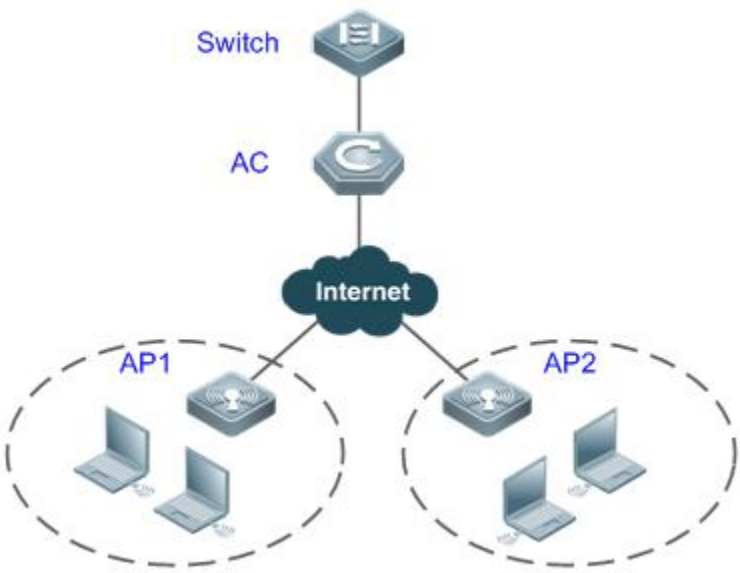
Application	Description
Fit AP Network Structure	This type of network consists of wired switches, ACs, and fit APs.

1.2.1 Fit AP Network Structure

Scenario

A fit AP network consists of wired switches, ACs, and fit APs. In the fit AP network structure, APs serve as the simple wireless access points and do not have the management or control function. The AC manages all the APs in a centralized manner, and pushes control policies to APs, and it is not necessary to configure APs one by one. As shown in Figure 1-1, the AC is connected to multiple APs through the CAPWAP tunnels. Users only need to perform configuration management on all the connected APs through the AC.

Figure 1- 1 Simple fit AP network topology



Remarks	AP1 and AP2 are AP devices in fit AP mode.

Deployment

- Configure a meaningful name for each AP so that the AP can be configured based on the name.
- Create a WLAN and configure WLAN-related properties.
- Create an AP group and add APs to a specified AP group so that all the APs in this AP group can be configured in a centralized manner through the AP group.
- Deploy the WLAN on all the APs in the AP group through configuration of the AP group, after which the APs can provide the WLAN access service for external entities and wireless terminals users can access the WLAN.

1.3 Features

Basic Concepts

AP

AP is an access point used by wireless terminals to access a wired network. It is equivalent to a bridge for communication between wireless terminals and a wired network.

AC

AC is a wireless access controller. It is connected with APs through the wired network to manage and control APs in a centralized manner.

AC Cluster

AC cluster is also called AC redundancy. With this function, multiple ACs with different priorities are designated for an AP. When the connection between the AP and a high-priority AC is down, the AP is connected to a low-priority AC (standby AC). When the connection with the high-priority AC is recovered, the AP disconnects the CAPWAP tunnel with the low-priority AC, and sets up a CAPWAP tunnel with the high-priority AC again.

Overview

Feature	Description
Configuration of AC Parameters	Configure parameters, such as the AC name and Trap message control.
Configuration of AP Parameters	Configure parameters, such as the AP name, Telnet user name and password, and periodical statistics report interval.
Configuration of AP Behaviors	Configure AP behaviors, including daily scheduled restart of an AP, restoration of AP factory settings, and AP reset.
AP Group Management	Manage APs through the AP group to reduce the workload incurred by configuring APs one by one.
AP Quantity Limit	Limit the maximum number of APs that can be connected to the AC.
AP Compliance Check	Implement the AP access control based on the bound MAC address.
AP Access Authentication	Authenticate the AP access.
AP Priority	Implement the AP access control based on the priority.
AC Cluster	Implement AC redundancy by using the AC cluster to reduce the AC single-point failure and improve availability of the wireless network.
WLAN Configuration	Configure a WLAN and deploy the WLAN on APs to provide network services for wireless users.
AP Backup	Configure the AP backup function to improve availability of the wireless network.

1.3.1 Configuration of AC Parameters

AC parameters include the AC name, Trap message control, and AC network access server (NAS) ID.

Working Principle

Configuration of AC parameters does not involve any working principle.

1.3.2 Configuration of AP Parameters

AP parameters include the AP name, Telnet user name and password, and periodical statistics report interval.

Working Principle

The AC configures AP parameters by pushing CAPWAP packets to an AP.

1.3.3 Configuration of AP Behaviors

AP behaviors include daily scheduled restart of an AP, restoration of AP factory settings, and AP reset.

Working Principle

Configuration of AP behaviors is implemented by pushing CAPWAP packets to an AP. The AP performs the related behaviors based on the configuration pushed by the AC.

1.3.4 AP Group Management

The AC manages APs through the AP group. All the APs in an AP group can be configured through the AP group, which reduces the configuration workload. Configurations of the AP group take effect on all the APs in the group. For the same configuration, if both the AP-based configurations and the AP-group-based configurations exist, the AP-based configurations prevail.

Working Principle

The system automatically creates a default AP group, which is named "default". By default, APs are added to the default group. You can create AP groups and add APs to these groups to manage APs by group.

1.3.5 AP Quantity Limit

The maximum number of APs that can be connected to an AC is configured to limit the maximum AP load of the AC, thus avoiding overload of the AC.

Working Principle

When the number of APs connected to the AC reaches the maximum number, no more APs can access the AC.

For the WALL-AP product series supplied by FS Network, each device is treated as 0.5 device when the maximum number of APs that can be connected to an AC is calculated. That is, the maximum number of WALL-APs that can be connected to an AC is twice the number of APs supported by the AC.

1.3.6 AP Compliance Check

The AP compliance check is also called AP access control based on the bound MAC address. If the AP compliance check is enabled, only APs with some specified MAC addresses are allowed to access the AC. This prevents access of unwanted APs and enhances security of the wireless network.

Working Principle

An AP is allowed to access the AC only when the AP configuration that is bound with the MAC address of this AP exists on the AC; otherwise, access of the AP to the AC is denied. To prevent binding MAC addresses with a large number of AP configurations, the MAC addresses of currently online APs are automatically bound when the AP compliance check is enabled. In addition, MAC addresses can be bound with specified AP configurations.

1.3.7 AP Access Authentication

AP access authentication can be implemented based on the serial number, password, or certificate. With the AP access authentication function, only authorized APs can access the AC.

Working Principle

When an AP sends an access request to the AC and uploads the authentication information, the AC verifies the authentication information. Only the AP that is successfully authenticated can access the AC.

1.3.8 AP Priority

The AP priority function is an advanced version of the AP quantity limit function. With this function, when the current number of APs connected to the AC reaches the upper limit, if a high-priority AP sends an access request, the AC proactively forces a low-priority AP to go offline and allows the access of the high-priority AP.

Working Principle

When an AP sends an access request, the current number of APs connected to the AC reaches the upper limit, and the AP priority function is enabled, the AC first compares the priorities. If the priority of an online AP is lower than the requesting AP, the AC forces a low-priority AP to go offline and allows the access of the high-priority AP.

1.3.9 AC Cluster

On the one hand, the AC cluster function enhances reliability of the AC cluster. On the other hand, this function controls the home AC of APs in stable conditions based on the priority to facilitate AP management.

Working Principle

See the CAPWAP protocol in RFC5415.

1.3.10 WLAN Configuration

Create and deploy a WLAN on an AP so that the AP can provide the WLAN access service for external entities.

Working Principle

The WLAN created on the AC is used for WLAN parameter configuration. The WLAN deployment information and parameters are pushed through the packets defined in the CAPWAP protocol.

1.3.11 AP Backup

The AP backup function is used to back up radio signals transmitted by APs that are physically adjacent with each other, have overlapped coverage, and transmit different radio signals. When an AP that transmits important radio signals is faulty, one or more standby APs transmit radio signals of the faulty AP to replace the faulty AP, thus ensuring stability of radio signals transmitted by devices supplied by FS Networks. This function is generally used in special scenarios. For example, in the zero roaming scenario of the medial industry, the AP4210 with a wide coverage is an important AP, and the APD-M within the coverage of the AP4210serves as a standby AP of the AP4210.

Working Principle

An AP backup group is created on the AC. In this AP backup group, one AP is selected as the active AP, and other APs are standby APs. When the active AP is faulty and goes offline, the WLAN configuration of the active AP is sent to all the standby APs in the group so that the standby APs can transmit radio signals of the active AP.

1.4 Configuration

Configuration	Description and Command	
Configuring an AC Name	(Optional) A meaningful name can be configured for the AC to facilitate management.	
	ac-name	Configures the name of the local AC.
Configuring the Trap Message Control Function	(Optional) It is used to enable sending of Trap messages. Network operation and maintenance (O&M) can be implemented based on the received Trap messages.	
	acctrl-trap	Configures whether the AC sends specified Trap messages.
Configuring the NAS ID of an AC	(Optional) By default, the NAS ID is the MAC address of the AC in dotted decimal notation.	
	nas-id	Configures the NAS ID of the AC in AC configuration mode.
Creating an AP Configuration	(Optional) It is used to create an AP configuration to configure a specified AP.	
	ap-config	Adds an AP configuration, or enter the AP configuration mode.
Creating an AP Group	(Optional) In AP group configuration mode, this command takes effect on all the online APs in the AP group.	

Configuration	Description and Command	
	ap-group	Adds an AP group configuration, or enters the AP group configuration mode.
Configuring the AP Group of an AP	(Optional) It is used to configure the AP group of a specified AP in AP configuration mode. By default, an AP belongs to the default group.	
	ap-group	Configures the AP group of an AP.
Configuring an AP Name	(Optional) A new name can be configured for an AP according to requirements.	
	ap-name	Configures an AP name.
Binding an MAC Address with an AP Configuration	(Optional) It is used to bind an MAC address with an AP configuration so that the AP configuration can take effect on the AP with the MAC address.	
	ap-mac	Binds an MAC address with an AP configuration.
Configuring the User Name and Password of an AP	(Optional) It is used to modify the Telnet user name and password of an AP according to requirements.	
	credential	Configures the user name and password of an AP.
Configuring the Interval at Which the AP Reports Statistics	(Optional) According to the standard, the AP reports statistics at the interval of 120s by default. The interval can be configured according to requirements.	
	statistics-timer	Configures the interval at which the AP reports statistics.
Configuring the Daily Scheduled Restart Time for an AP	(Optional) The daily scheduled restart function can be configured for an AP to prevent the AP from working for a long time.	
	reload at	Configures the daily scheduled restart time for an AP.
Restoring Factory Settings of a Specified AP	(Optional) It is used to restore factory settings of an AP.	
	factory-reset	Restores factory settings of a specified AP.
Resetting an AP	(Optional) It is used to reset an AP.	
	reset	Resets an AP.
Configuring the AP Quantity Limit	(Optional) The maximum number of APs connected to the AC can be configured according to requirements to reduce the maximum load of the AC.	
	wtp-limit	Configures the maximum number of APs that can be connected to the AC.
Configuring the AP Compliance Check	(Optional) The AP compliance check can be enabled to allow the access of only APs with the bound MAC addresses, thus effectively controlling the access of APs.	
	bind-ap-mac	Enables or disables the AP compliance check in AC configuration mode.
Configuring AP Access Authentication	(Optional) AP access authentication can be configured so that only authorized APs can access the AC, which enhances security of the wireless network.	
	ap-auth enable	Enables or disables the AP access authentication function of the AC in AC configuration mode.
	ap-auth serial-update	Updates authentication serial numbers for all online APs in AC

Configuration	Description and Command	
		configuration mode.
	ap-auth	Configures the access authentication information of an AP in AP configuration mode.
Configuring the AP Priority	(Optional) This command is available in both the AC and AP configuration modes.	
	ap-priority	Enables or disables the AP access priority function of the AC in AC configuration mode.
	priority	Configures the failover priority of a specified AP in AP configuration mode.
Configuring the AP System Log Information	(Optional) It is used to configure the log information of a specified AP or all APs in AP configuration mode.	
	logging on	Enables or disables the function of displaying system logs.
	logging server	Configures the address of the system logging server.
Creating a WLAN	(Optional) A WLAN must be created before it can be deployed.	
	wlan-config	Creates a WLAN, or enters the WLAN configuration mode.
Deploying a WLAN	(Optional) It is used to configure the WLAN-VLAN mapping of a specified AP group and deploy the WLAN on all the APs in the AP group.	
	interface-mapping	Configures the WLAN-VLAN mapping of a specified AP group in AP group configuration mode.
Enabling or Disabling WLAN SSID Broadcasting	(Optional) SSID broadcasting is disabled by default.	
	enable-broad-ssid	Enables or disables SSID broadcasting of a specified WLAN in WLAN configuration mode.
Configuring the NAS ID of WLAN Users	(Optional) The NAS ID is a null string by default.	
	nas-id	Configures the NAS ID of a specified WLAN user.
Configuring the WLAN SSID Name	(Optional) A new SSID can be configured for the WLAN according to requirements.	
	ssid	Modifies the SSID name of the WLAN in WLAN configuration mode.
Configuring the AP Backup Function	(Optional) It is used to improve availability of the wireless network.	
	ap-backup group	Creates an AP backup group in AC configuration mode.
	ap-backup-group	Binds an AP backup group.
Configuring the Default SSID	**offline-ssid**	Configures the WLAN access signal provided when an AP is offline.

-

1.4.1 Configuring an AC Name

Configuration Effect

- Set the name of an AC to a specified string.

Notes

- The AC name is a string of 1 to 63 characters, and cannot contain any space.

Configuration Steps

- Optional. Run the **ac-name** *ac-name* command in AC configuration mode to configure a new name for an AC.
- Run the **ac-controller** command to enter the AC configuration mode.
- Run the **ac-name** command to configure an AC name in AC configuration mode on an AC device.

Command	**ac-controller**
Parameter Description	N/A
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**ac-name***ac-name* **no ac-name**
Defaults	The default AC name is FS_Ac_*Last six digits of MAC address*. For example, if the MAC address of an AC is 001a.a916.e7b8, the default name of this AC is FS_Ac_16e7b8.
Parameter Description	*ac-name*: indicates the name of an AC. The name is a string of 1 to 63 characters, and cannot contain any space.
Command Mode	AC configuration mode
Usage Guide	Different names can be configured for different ACs to facilitate management.

Verification

- Run the **show ac-config** command to check the current AC name and determine whether the configuration is successful.

Configuration Example

Configuring the Name of an AC as "FS-AC1"

Configuration Steps	• Enter the AC configuration mode. • Configure an AC name. • Use the **no** form of this command to restore the default AC name.
AC	FS(config)#ac-controller FS(config-ac)# FS(config-ac)#ac-name FS-AC1 FS(config)#ac-controller FS(config-ac)#no ac-name
Verification	Run the **show ac-config** command to check the current AC name.

AC	FS#show ac-config ac_name :FS-AC1

Common Errors

- N/A

1.4.2 Configuring the Trap Message Control Function

Configuration Effect

- The AC sends the following types of Trap messages: CAPWAP tunnel up/down information, failures to add APs to the AC,CAPWAP tunnel packet decryption failures, upgrade failures, time synchronization failures, and STA online/offline information.
- By default, all the preceding Trap messages are not sent. You can run the **acctrl-trap** command in AC configuration mode to enable sending of specified Trap messages.

Notes

- N/A

Configuration Steps

- Optional. On the AC device, enter the AC configuration mode and run the **acctrl-trap** command to configure the Trap message control function.

Command	**acctrl-trap**[**acap-updown-ctrl** | **acap-joinfail-ctrl** | **acap-decryeroreport-ctrl** | **acap-imageupdt-ctrl** | **acap-timestamp-ctrl** | **acsta-oper-ctrl**]
Parameter Description	**acap-updown-ctrl**: Determines whether to send the Trap messages that contain the CAPWAP tunnel up/down information. **acap-joinfail-ctrl**: Determines whether to send the Trap messages that contain information about failures of adding APs to the AC. **acap-decryeroreport-ctrl**: Determines whether to send the Trap messages that contain information about CAPWAP tunnel packet decryption failures. **acap-imageupdt-ctrl**: Determines whether to send the Trap messages that contain information about the **bin** file upgrade failures of the AP. **acap-timestamp-ctrl**: Determines whether to send the Trap messages that contain the time synchronization information. **acsta-oper-ctrl**: Determines whether to send the Trap messages that contain the STA online/offline information.
Defaults	By default, all types of Trap messages are not sent. You can run the **acctrl-trap** command in AC configuration mode to enable sending of these messages.
Command Mode	AC configuration mode
Usage Guide	This command is used to control sending of Trap messages on the AC.

Verification

- Run the **show ac-config** command to check the sending status of various types of Trap messages.

Configuration Example

Enabling the AC to Send the Trap Messages That Contain Information About Failures to Add APs to the AC

Configuration Steps	• Enter the AC configuration mode. • Enable the AC to send the Trap messages that contain information about failures to add APs to the AC. • Use the **no** form of this command to restore the default setting.
AC	FS(config)#ac-controller FS(config-ac)#acctrl-trap acap-joinfail-ctrl FS(config)#ac-controller FS(config-ac)#no acctrl-trap acap-joinfail-ctrl
Verification	Run the **show ac-config** command to check the sending status of various types of Trap messages.
AC	FS#show ac-config acctrl-trap acap-updown-ctrl :Disable acctrl-trap acap-joinfail-ctrl :Enable acctrl-trap acap-decryeroreport-ctrl :Disable acctrl-trap acap-imageupdt-ctrl :Disable acctrl-trap acap-timestamp-ctrl :Disable acctrl-trap acsta-oper-ctrl :Disable

Common Errors

- N/A

1.4.3 Configuring the NAS ID of an AC

Configuration Effect

- On the WLAN, the NAS IDs identify different hot spot areas. By default, the NAS ID of an AC is the MAC address of the AC in dotted decimal notation.

Notes

- N/A

Configuration Steps

- Optional.
- On the AC device, enter the AC configuration mode and run the **nas-id** command to configure the NAS ID.

Command	**nas-id** *ac-nas-id*

	no nas-id
Parameter Description	N/A
Defaults	MAC address of the AC in dotted decimal notation
Command Mode	AC configuration mode
Usage Guide	N/A

Verification

- Run the **show running** command to check the AC configuration.

Configuration Example

Setting the NAS ID of the AC to 123456789

Configuration Steps	• Enter the AC configuration mode. • Configure the NAS ID.
AC	FS(config)# ac-controller FS(config-ac)#nas-id123456789
Verification	Run the **show running** command to check the AC configuration.
AC	FS#show running ! ac-controller nas-id 123456789 !

Common Errors

- N/A

1.4.4 Creating an AP Configuration

Configuration Effect

- Create an AP configuration with the specified name, and enter the AP configuration mode.
- If the AP configuration corresponding to a name already exists, you can directly enter the AP configuration mode after the command is executed.
- The *ap-name* parameter indicates the name of the AP configuration. When an AP gets online, the AP name uploaded by the AP is matched with the AP configuration name to determine the mapping relationship between the AP device and AP configuration.

Notes

- N/A

Configuration Steps

- Optional.
- On the AC device, enter the global configuration mode and run the **ap-config***ap-name* command to create an AP configuration.

Command	**ap-config** *ap-name*
Parameter Description	*ap-name*: indicates the name of the AP configuration.
Defaults	No AP configuration is created by default.
Command Mode	Global configuration mode
Usage Guide	1. You can run the **ap-config all** command to enter the all-AP configuration mode. Configurations made in this mode take effect on all APs associated with the current AC. Configurations made in AP configuration mode take precedence over configurations made in all-AP configuration mode. If configurations (non-default settings) exist in AP configuration mode (entered by running the **ap-config** *ap-name* command), such configurations are preferentially used; otherwise, configurations made in all-AP configuration mode (entered by running the **ap-config all** command) are used. 2. You can run the **no ap-config** *ap-name* command to delete a specified AP configuration. If the AP corresponding to this configuration is already online, the AP will be forced offline and then go online again after the configuration is deleted. 3. You can run the **no ap-config all** command to delete configurations of all offline APs on the current AC.

Verification

- Run the **show ap-config running** *ap-name* command to check the configurations of the AP.

Configuration Example

Creating an AP Configuration Named "FS_AP"

Configuration Steps	• Create an AP configuration named "FS_AP".
AC	FS(config)#ap-config FS_AP You are going to config AP(FS_AP), which is not on line now. FS(config-ap)#
Verification	Run the **show ap-config running** command to check the current configurations of the AP.
AC	FS#show ap-config running FS_AP ! ap-config FS_AP !

Common Errors

- N/A

1.4.5 Creating an AP Group

Configuration Effect

- The AC manages APs through the AP group. All the APs in an AP group can be configured through the AP group, which reduces the configuration workload. Configurations of the AP group take effect on all the APs in the group.

Notes

- The default group is created automatically by the system, and cannot be deleted.
- When an AP group is deleted, APs of this group are automatically moved to the default group.
- Configurations made in different configuration modes take effect in the following sequence: ap-config ap-name>ap-group>ap-config all.

Configuration Steps

- Optional.
- On the AC device, enter the global configuration mode, and run the **ap-group** *ap-group-name* command to create an AP group.

Command	**ap-group** *ap-group-name* **no ap-group** *ap-group-name*
Parameter Description	***ap-group-name***: indicates the name of an AP group.
Defaults	An AP group named "default" is automatically created by default after the system is started. This group can neither be created nor deleted.
Command Mode	Global configuration mode
Usage Guide	When the **no** form of the command is used to delete an AP group, APs of this group are automatically moved to the default group.

Verification

- Run the **show running** command to check configurations of all AP groups.

Configuration Example

Creating an AP Group Named "APG-1"

Configuration Steps	• In global configuration mode, run the **ap-group** command to create an AP group.
AC	FS(config)#ap-group APG-1 FS(config-ap-group)#
Verification	Run the **show running** command to check whether the AP group named "APG-1" exists.
AC	FS#show running ! ap-group APG-1

	!

Common Errors

- N/A

1.4.6 Configuring the AP Group of an AP

Configuration Effect

- An AP group must already exist if you want to add an AP to this group.
- By default, APs belong to the default AP group, that is, the AP group named "default".
- APs inherit all configurations of the AP group to which APs belong. If the same configuration exists in the specified AP configurations (**ap-config***ap-name*), all AP configurations (**ap-config all**), and AP group configurations, the configurations take effect in the following sequence: specified AP configurations > AP group configurations > all AP configurations. Therefore, if the AP group of an AP changes, AP group configurations inherited by this AP change as well.

Notes

- N/A

Configuration Steps

- Optional.
- Run the **ap-config** command to create an AP group or enter the AP configuration mode.
- On the AC device, enter the AP configuration mode and run the **ap-group** command to configure the AP group of an AP.

Command	**ap-config***ap-name*
Parameter Description	*ap-name*: indicates the name of the AP configuration.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**ap-group** *ap-group-name* **no ap-group**
Parameter Description	*ap-group-name*: indicates the name of an AP group.
Defaults	By default, APs are automatically added to the default group.
Command Mode	AP configuration mode
Usage Guide	When an AP group is deleted, APs of this group are automatically moved to the default group.

Verification

- Run the **show ap-config running** command to check the current configurations of the AP.

Configuration Example

Configuring the AP Group to Which FS-AP1 Belongs

Configuration Steps	● Create an AP group named "apg-1". ● Enter the AP configuration mode. ● Use the **no** form of this command to restore the default AP group, that is, the AP group named "default".
AC	FS(config)#ap-group apg1 FS(config-ap-group)# FS(config)#ap-config FS-AP1 FS(config-ap)# FS(config-ap)#ap-group apg-1 FS(config)#ap-config FS-AP1 FS(config-ac)#no ap-group
Verification	Run the **show ap-config running** command to check the current configurations of the AP.
AC	FS(config)#show ap-config running FS-AP1 ! ap-config FS-AP1 ap-group apg-1 !

Common Errors

- N/A

1.4.7 Configuring an AP Name

Configuration Effect

Configure an AP name on the AC.

- If the AP is currently online, the configuration of the AP name takes effect immediately. In addition, the AP name in the specified AP configuration mode (that is, the string next to **ap-config**) is immediately replaced by the new name.
- If the AP is currently offline, the configuration of the AP name takes effect after the AP goes online, and the AP name in the AP configuration mode is not replaced by the new name until the AP goes online.
- After the AP name is configured, you can continue to configure this AP without exiting from the AP configuration mode.
- If the corresponding AP is online, the **no** form of the command is not supported.
- If the corresponding AP is online, the **no** form of the command can be used to delete the AP name configuration that is currently not effective.
- If the new name is already in use, the configuration fails.

Configure an AP name on the AP.

- If the CAPWAP connection is not set up, the AP name is configured directly.

- If the CAPWAP connection is set up, the AP name is configured first. Then the CAPWAP tunnel will be torn down and a connection will be set up again. If the AP name is already configured on the AC or configured offline, this AP name prevails.

Notes

- The AP name is a string of 1 to 63 characters, and cannot contain any space.
- The AP name cannot be configured as "all" or "AP".
- Avoid configuring the same AP name for different offline APs. If the same AP name is configured for different offline APs, the new name takes effect on the AP that goes online first, and the APs that go online later still use the original names.
- Configuring the AP name on the AP only takes effect in fit AP mode.

Configuration Steps

- Optional. You can run the **ap-name** *ap-name* command in AP configuration mode to configure an AP name. It is recommended that a meaningful AP name be configured to facilitate management.
- On the AC device, enter the AP configuration mode and run the **ap-group** command to configure an AP name.

Command	**ap-name** *name*
Parameter Description	*name*: indicates the name of an AP. The name cannot contain any space.
Defaults	The AC uses the name uploaded by the AP as the AP name. In the factory settings, the MAC address is often used as the name of an AP.
Command Mode	AP configuration mode
Usage Guide	1. Do not configure the AP name as "all" or "AP". 2. After the command is executed, the command mode of an online AP is the AP command mode with the new AP name, and you can continue to configure other properties of the AP without existing from the command mode. The command mode of an offline AP remains unchanged.

- On the AP device, enter the global configuration mode and run the **ap-name** command to configure an AP name.

Command	**ap-name** *name*
Parameter Description	*name*: indicates the name of an AP. The name cannot contain any space.
Defaults	The default name is AP.
Command Mode	Global configuration mode
Usage Guide	1. Do not configure the AP name as "all". 2. After this command is executed, the CAPWAP tunnel will be set up again.

Verification

- Run the **show ap-config running** command to check the current configurations of the AP.
- Run the **show ap-config summary** command to check whether the name of the online AP is the new name.

- Run the **show running-config** command to check the AP configuration.

Configuration Example

Changing the Name of an Online AP from "FS-AC1" to "FS-AC2"

Configuration Steps	● Enter the AP configuration mode. ● Configure the name of an AP.
AC	FS(config)#ap-config FS-AC1 FS(config-ap)#ap-name FS-AC2
Verification	● Run the **show ap-config running** command to check the current configurations of the AP. ● Run the **show ap-config summary** command to query the current name of the online AP.
AC	FS#show ap-config running ! ap-config FS-AC2 ! FS#show ap-config summary ========= show ap status ========= Radio: Radio ID or Band: 2.4G = 1#, 5G = 2# E = enabled, D = disabled, N = Not exist Current Sta number/Max Sta number supported Channel: * = Global Power Level = Percent Online AP number: 0 Offline AP number: 1 AP Name IP Address Mac Address Radio 1 Radio 2 Up/Off time State ---------- ---------- ---------- ---------- ---------- ---------- ----- ap1 10.0.20.15 00d0.f822.33b0 N -/- - - N -/- - - 0:00:16:03 Quit

Changing the Name of an Offline AP from "FS-AC1" to "FS-AC2"

Configuration Steps	● Enter the AP configuration mode. ● Configure the name of an AP.
AC	FS(config)#ap-config FS-AC1

	FS(config-ap)#ap-name FS-AC2
Verification	Run the **show ap-config running** command to check the current configurations of the AP.
AC	FS#show ap-config running ! ap-config FS-AC1 ap-name FS-AC2 !

Deleting the Name Configuration of an Offline AP FS-AC1

Configuration Steps	● Enter the AP configuration mode. ● Delete the name configuration of an offline AP FS-AC1.
AC	FS(config)#ap-config FS-AC1 FS(config-ap)#no ap-name
Verification	Run the **show ap-config running** command to check the current configurations of the AP.
AC	FS#show ap-config running ! ap-config FS-AC1 !

Configuring the Name of an AP as FS-AP1.

Configuration Steps	● Enter the global configuration mode. ● Configure the AP name.
AP	FS(config)#ap-name FS-AP1
Verification	Run the **show ap-config running** command to check the current configurations of the AP.
AP	FS#show running-config Building configuration... Current configuration: 1592 bytes version 11.1(5)B0 privilege exec all level 1 debug privilege exec all level 1 show privilege exec all level 1 terminal privilege exec all level 1 undebug ap-name FS-AP1 fair-schedule !

Common Errors

- N/A

1.4.8 Binding an MAC Address with an AP Configuration

Configuration Effect

- In AP configuration mode, run the **ap-mac** command to bind an MAC address with an AP configuration so that the AP configuration takes effect only on the AP with the MAC address.
- Generally, when an AP goes online, it determines the configuration to be used based on the mapping between the AP name and the AP configuration name. MAC address binding is a stronger binding relationship than name mapping, and takes precedence over name mapping. Therefore, when an AP goes online, the AP uses the configuration so far as the MAC address bound with the AP configuration is the same as the MAC address of the AP.
- If no MAC address is bound with an AP configuration, the MAC address is automatically bound when the corresponding AP goes online. This bounding relationship still takes effect when the AP goes offline. That is, the binding configuration will be automatically generated when the AP goes online.
- MAC address binding is also used for the AC access control function configured by using the **bind-ap-mac** command. For details, see the configuration description of this command.
- You can bind a specified MAC address only with the configuration of an offline AP.

Notes

- You can bind a specified MAC address only with the configuration of an offline AP.

Configuration Steps

- Optional.
- On the AC device, enter the AP configuration mode and run the **ap-mac** command to bind an MAC Address with an AP configuration.

Command	**ap-mac** *ap-mac-address* **no ap-mac**
Parameter Description	*ap-mac-address*: indicates the MAC address that is bound.
Defaults	No AP configuration is bound with the MAC address by default. You can bind the MAC address of an AP with the AP configuration to forcibly apply this AP configuration on the AP with the MAC address.
Command Mode	AP configuration mode
Usage Guide	• The **ap-mac** *ap-mac-address* command is applicable to configurations of offline APs. You can use this command to specify the MAC address of an offline AP so that the AP configuration can be located directly based on the MAC address after the AP goes online. • The **no ap-mac** command is applicable to all AP configurations.

Verification

- Run the **show ap-config running** command to check the MAC address binding of the current AP.

Configuration Example

Binding the Offline AP FS-AP1 with the MAC Address 001a.a979.1234

Configuration Steps	● Enter the AP configuration mode. ● The **no** form of the command is used to delete the MAC address binding.
AC	FS(config)#ap-config FS-AP1 FS(config-ap)#ap-mac 001a.a979.1234 FS(config)#ap-config FS-AP1 FS(config-ac)#no ap-mac
Verification	Run the **show ap-config running** command to check the current configurations of the AP.
AC	FS(config)#show ap-config running FS-AP1 ! ap-config FS-AP1 ap-mac 001a.a979.1234 !

Common Errors

- N/A

1.4.9 Configuring the User Name and Password of an AP

Configuration Effect

- Authorized users may directly login to an AP and modify the AP configuration through Telnet, which affects normal running of the WLAN. To prevent this problem, you can configure the Telnet user name and password of a specified AP.
- The **credential** command can be used in **ap-config** *ap-name*, **ap-group**, or **ap-config all** configuration mode. Configurations made by using the **credential** command take effect in the following sequence: **ap-config** *ap-name*>**ap-group**>**ap-config all**.

Notes

- N/A

Configuration Steps

- Optional: You can run the **credential** *user-name password* command to configure a new Telnet user name and password in AP configuration mode to enhance security.
- On the AC device, enter the AP or AP group configuration mode and run the **credential** command for configuration.

Command	**credential** *user-name password* **nocredential**
Parameter Description	*user-name*: indicates the user name. A user name cannot contain any space. *password*: indicates the password. A password cannot contain any space.
Defaults	The AC device uses factory settings of the Telnet user name and password of an AP. You can modify the Telnet user name and password of an AP according to requirements to facilitate management.

Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	N/A

Verification

- Run the **show ap-config running** or **show running** command to check the configurations.

Configuration Example

Configuring the User Name and Password of FS-AP1

Configuration Steps	• Configure the user name and password of FS-AP1. • Use the **no** form of the command to delete the configuration of the user name and password of the AP. (After the deletion, the default user name and password are restored on the AP.)
AC	FS(config)#ap-config FS-AP1 FS(config-ap)#credential user pass FS(config)#ap-config FS-AP1 FS(config-ac)#no credential
Verification	Run the **show ap-config running** command to check the current configurations of the AP.
AC	FS(config)#show ap-config running FS-AP1 ! ap-config FS-AP1 credential user pass !

Common Errors

- N/A

1.4.10 Configuring the Interval at Which the AP Reports Statistics

Configuration Effect

- Run the **statistics-timer** command to configure the interval at which the AP reports statistics.

Notes

- N/A

Configuration Steps

- Optional. You can adjust the interval based on the statistics accuracy requirement and loads on the AC and AP.
- On the AC device, enter the AP or AP group configuration mode and run the **statistics-timer** command for configuration.

Command	**statistics-timer** *timer-interval* **nostatistics-timer**

Parameter Description	*timer-interval*: indicates the interval that the AP reports statistics. The unit is second.
Defaults	120s
Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	N/A

Verification

- Run the **show ap-config running** command to check the configurations.

Configuration Example

Setting the Interval at Which FS-AP1 Reports Statistics to 300s

Configuration Steps	• Set the interval at which FS-AP1 reports statistics to 300s. • Use the **no** form of the command to restore the default interval at which FS-AP1 reports statistics.
AC	FS(config)#ap-config FS-AP1 FS(config-ap)#statistics-timer 300 FS(config)#ap-config FS-AP1 FS(config-ac)#no statistics-timer
Verification	Run the **show ap-config running** command to check the current configurations of the AP.
AC	FS(config)#show ap-config running FS-AP1 ! ap-config FS-AP1 statistics-timer 300 !

Common Errors

- N/A

1.4.11 Configuring the AP System Log Information

Configuration Effect

- Control displaying of the AP system logs, and set the IP address of the server that records the AP system logs.

Notes

- N/A

Configuration Steps

- Optional.
- Run the **logging on** command to display system logs of a specified AP.
- Run the ***logging server*** *ip-address* ***[udp-port*** *num]* command to configure the IP address of the system log server of a specified AP.

Command	**loggingon** **no loggingon**
Parameter Description	N/A
Defaults	The system logs are displayed by default.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	N/A

Command	**logging server** *ip-address*[**udp-port** *num*] **no logging server** *ip-address*
Parameter Description	*ip-address*: indicates the IP address of the host that receives the log information. num: indicates the ID of the port on the host that receives the log information. This parameter is optional.
Defaults	N/A
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	You can configure at most five log server addresses. The log information will be sent simultaneously to all the configured log servers.

Verification

- Run the **show ap-config running** command to check the configurations.

Configuration Example

Disabling the Function of Displaying System Logs on FS-AP1

Configuration Steps	• Enter the AP configuration mode. • Disable the function of displaying system logs.
AC	FS(config)#ap-config FS-AP1 FS(config-ap)#no logging on
Verification	Run the **show ap-config running** command to check the current configurations of the AP.
AC	FS(config)#show ap-config running FS-AP1 ! ap-config FS-AP1 no logging on !

Configuring the Log Server Address of FS-AP1

Configuration Steps	• Enter the AP configuration mode. • Set the log server address to 1.1.1.1.
AC	FS(config)#ap-config FS-AP1

	FS(config-ap)#logging server 1.1.1.1
Verification	Run the **show ap-config running** command to check the current configurations of the AP.
AC	FS(config)#show ap-config running FS-AP1 ! ap-config FS-AP1 logging server 1.1.1.1 !

Common Errors

- N/A

1.4.12 Configuring the Daily Scheduled Restart Time for an AP

Configuration Effect

- If APs work too long, the load may be too heavy, affecting the network access quality of users. To prevent this problem, you can configure the daily scheduled restart time for an AP so that the network access quality of users can be ensured every day.

Notes

- N/A

Configuration Steps

- Optional. You can enable the daily scheduled restart function based on the AP load.
- Configure the daily scheduled restart time to prevent APs from working for a long time, enhancing availability of the network.

Command	**reload at** *time* **no reload at**
Parameter Description	*time*: indicates the time when the AP is restarted every day. The time is expressed in the format of hh:mm:ss.
Defaults	The daily scheduled restart function of an AP is disabled by default.
Command Mode	AP configuration mode
Usage Guide	N/A

Verification

- Run the **show ap-config running** command to check the configurations.

Configuration Example

Enabling FS-AP1 to Restart at 1:00:00 Every Day

Configuration Steps	• Enable FS-AP1 to restart at 1:00:00 every day. • Use the **no** form of the command to cancel the scheduled restart configuration.
AC	FS(config)#ap-config FS-AP1

	FS(config-ap)#reload at 1:00:00 FS(config)#ap-config FS-AP1 FS(config-ac)#no reload at
Verification	Run the **show ap-config running** command to check the current configurations of the AP.
AC	FS(config)#show ap-config running FS-AP1 ! ap-config FS-AP1 reload at 1:00:00 !

Common Errors

- N/A

1.4.13 Restoring Factory Settings of a Specified AP

Configuration Effect

- Restore factory settings of a specified AP.
- The configuration takes effect only on an online AP.

Notes

- This operation will cause offline and reset of the AP.

Configuration Steps

- Optional. You can restore factory settings of a specified AP according to requirements.
- Restoring AP factory settings is an instant behavior of an AP. This command can restore factory settings of the AP and will trigger reset of the AP.

Command	**factory-reset***ap-name*
Parameter Description	*ap-name*: indicates the name of an AP.
Defaults	N/A
Command Mode	AC configuration mode
Usage Guide	This operation will cause reset of the AP.

Verification

- After this command is executed for an online AP, this AP will go offline. After the AP goes online again, run the **show ap-config running** command to check whether factory settings of the AP are restored.

Configuration Example

Restoring Factory Settings of the Online AP FS-AP1

Configuration Steps	● Enter the AC configuration mode. ● Restore factory settings of the online AP FS-AP1.
AC	FS(config)#ac-controller FS(config-ac)#factory-reset FS-AP1
Verification	After this command is executed for an online AP, this AP will go offline. After the AP goes online again, run the **show ap-config running** command to check whether factory settings (null settings) of the AP are restored.

Common Errors

- N/A

1.4.14 Resetting an AP

Configuration Effect

- Reset an online AP.
- Reset all online APs.

Notes

- N/A

Configuration Steps

- Optional. You can reset one or more APs according to requirements.
- If you configure AP reset on the AC, the corresponding AP will reset. You can configure reset of a specified AP or all online APs.

Command	**reset**{ **all** |**single** *ap-name*}
Parameter Description	**all**: indicates that all online APs are reset. **single** ***ap-name***: indicates that a specified AP is reset.
Defaults	N/A
Command Mode	AC configuration mode
Usage Guide	N/A

Verification

- After the configuration is completed, you can view the syslog record on the AC, indicating that the corresponding AP goes offline, and the AP will be reset.

Configuration Example

Resetting FS-AP1

Configuration Steps	● Enter the AC configuration mode. ● Reset FS-AP1.
AC	FS(config)#ac-controller FS(config-ac)#

	FS(config-ac)#reset FS-AP1
Verification	Check whether FS-AP1 is reset, and whether the following syslog record indicating the offline event of the AP can be viewed on the AC.
AC	%APMG-6-RX_CTRL_MSG: AP(AP_20#3F_S:001a.a912.3456) leave AC.

Common Errors

- N/A

1.4.15 Configuring the AP Quantity Limit

Configuration Effect

- The number of online APs connected to the AP does not exceed the configured maximum number of APs supported by the AC.

Notes

- The weight of an AP varies according to the AP model. For example, the weight of one WALL-AP is 0.5 and two WALL-APs are treated as one AP. When APs are connected to an AC, the weighted number of APs is calculated based on the weight.

Configuration Steps

- Optional. You can configure the AP quantity limit within the capacity range according to requirements.

Command	**wtp-limit** *max-num*
Parameter Description	*max-num*: indicates the maximum number of APs that can be connected to an AC.
Defaults	By default, this number is equal to the number of APs supported by an AC.
Command Mode	AC configuration mode
Usage Guide	This command is used to configure the maximum number of APs connected to an AC.

Verification

- Run the **show ac-config** command to check the current AC name and determine whether the configuration is successful.

Configuration Example

Setting the Maximum Number of APs Connected to the AC to 512

Configuration Steps	• Enter the AC configuration mode. • Set the maximum number of APs connected to the AC to 512. • Use the **no** form of this command to restore the default setting.
AC	FS(config)#ac-controller FS(config-ac)#wtp-limit 512 FS(config)#ac-controller FS(config-ac)#no wtp-limit
Verification	Run the **show ac-config** command to check the configured maximum number of APs that can be connected to the AC.

AC	FS#show ac-config … max_wtp :512 …

Common Errors

- N/A

1.4.16 Configuring the AP Compliance Check

Configuration Effect

- The AP compliance check is also called AP access control based on the bound MAC address, or bind-ap-mac function. If AP compliance check is enabled, only APs that have offline configurations bound with their MAC addresses are allowed to associate with the AC.

Notes

- N/A

Configuration Steps

- Optional. You can enable the AP compliance check to allow only APs with specified MAC address to go online, thus implementing strict control on access of APs.
- When the AP compliance check is enabled, all online APs are automatically bound with MAC addresses. Therefore, it is recommended that this function be disabled during network deployment, and enabled after all APs within the plan go online.
- When the **bind-ap-mac** function is enabled, MAC addresses automatically bound with all online APs are converted to the formal MAC address binding, which is not automatically deleted when APs go offline.
- On the AC device, you can run the **ap-mac** *X.Y.Z* command in AP configuration mode to configure the MAC address binding of an individual AP configuration.

Command	**bind-ap-mac** **no bind-ap-mac**
Parameter Description	N/A
Defaults	The AP compliance check is disabled by default.
Command Mode	AC configuration mode
Usage Guide	This command is used to enable the AP compliance check.

Command	**ap-mac** *ap-mac-address* **no ap-mac**
Parameter Description	*ap-mac-address*: indicates the MAC address that is bound.
Defaults	N/A

Command Mode	AP configuration mode
Usage Guide	The **ap-mac***ap-mac-address* command is applicable to offline APs. You can use this command to specify the MAC address of an offline AP so that the AP configuration can be located directly based on the MAC address after the AP goes online.

Verification

- Run the **show running** command to check whether the **bind-ap-mac** function is enabled.
- Run the **show ap-config running** command to check the MAC address binding information of AP configurations.

Configuration Example

Enabling the bind-ap-mac Function on an AC

Configuration Steps	● After all authorized APs go online, enter the AC configuration mode and run the **bind-ap-mac** command to enable the bind-ap-mac function.
AC	FS(config)#ac-controller FS(config-ac)#bind-ap-mac
Verification	Run the **show running** command to check whether the bind-ap-mac function is enabled.
AC	FS#show running ! ac-controller bind-ap-mac !

Common Errors

- N/A

1.4.17 Configuring AP Access Authentication

Configuration Effect

- AP access authentication can be implemented based on the serial number, password, or certificate.

Notes

- If you run the **ap-auth** { **serial** | **password** | **certificate** } **enable** command in AC configuration mode to enable the access authentication function, but do not run the **ap-auth** { **serial** *serial-string* |**password** *password* |**ac-cert** *ac-cert-name* |**ap-cert** *ap-cert-name* } command in AP configuration mode to configure related authentication parameters, AP access authentication will fail and the AP cannot go online.

Configuration Steps

- Optional.
- Run the **ap-auth serial-update** command to update the authentication serial numbers for all online APs.

- Run the **ap-auth enable** command in AC configuration mode to enable a specified type of AP access authentication.
- Run the **ap-auth** { **serial** *serial-string*|**password** *password* |**ac-cert** *ac-cert-name* |**ap-cert** *ap-cert-name* } command to configure the related AP access authentication parameters.

Command	**ap-auth serial-update**
Parameter Description	N/A
Defaults	This function is disabled by default.
Command Mode	AC configuration mode
Usage Guide	All online APs use the current AP serial numbers for authentication.

Command	**ap-auth** {**serial** |**password** |**certificate**} **enable**
Parameter Description	**serial**: indicates the authentication function based on the AP access serial number. **password**: indicates the authentication function based on the AP access password. **certificate**: indicates the authentication function based on the AP certificate.
Defaults	The authentication function is disabled by default.
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**ap-auth**{**serial** *serial-string*|**password** *password* |**ac-cert** *ac-cert-name*|**ap-cert** *ap-cert-name*}
Parameter Description	*serial-string*: indicates the AP access serial number. *password*: indicates the AP access password. *ac-cert-name*: indicates the AC certificate file name. *ap-cert-name*: indicates the AP certificate file name.
Defaults	This function is disabled by default.
Command Mode	AP configuration mode
Usage Guide	The AP access authentication configurations take effect only when the AP makes an access attempt. If the AP is already online, the configurations take effect next time when the AP goes online. The **ap-auth serial** command cannot be used in all-AP configuration mode because the serial number varies according to the AP. The certificate file issued by the **ap-auth ap-cert** command will be stored as **cert.crt** on the AP, and the file name cannot be changed.

Verification

- Run the **show ap-config running** command to check whether the configuration is successful.

Configuration Example

Configuring the AP Access Authentication Function Based on the Serial Number

Configuration	• After all authorized APs go online, update the authentication serial numbers for all online APs.

Steps	● Enable the AP access authentication function based on the serial number. ● Configure the authentication serial number of a specified AP.
AC	FS(config)#ac-controller FS(config-ac)#ap-auth serial-update FS(config)#ac-controller FS(config-ac)#ap-auth serial enable FS(config)#ap-config FS-AP1 FS(config-ap)#ap-auth serial G1GD10U000456
Verification	Run the **show running** or **show ap-config running** command to check the AP access authentication configurations.

AC	FS(config)#show run
	!
	ac-controller
	  ap-auth serial enable
	!
	FS(config)#show ap-config running FS-AP1
	!
	ap-config FS-AP1
	  ap-auth serial G1GD10U000456
	!

Updating the Access Authentication Certificate of an AP

Configuration Steps	● Update the access authentication certificate of an AP.
AC	FS(config)#ap-config FS-AP1 FS(config-ap)#ap-auth ap-cret ap1_cret.crt
Verification	Run the **show ap-config running** command to check the name of the current AC. If the corresponding AP is online, the **ap1_cret.crt** file is updated to the AP instantly; otherwise, the file is updated to the AP after the AP goes online.
AC	FS(config)#show ap-config running FS-AP1 ! ap-config FS-AP1 ap-auth ap-cret ap1_cret.crt !

Common Errors

- N/A

1.4.18 Configuring the AP Priority

Configuration Effect

- By default, the AC allows the access of APs based on the sequence of AP association requests received by the AC. You can set the failover priorities of APs and enable the AC to support the failover priorities of APs so that the AC can allow the access of APs based on the AP priorities. The AP priority ranges from 1 to 4, where 1 is the lowest priority.

Notes

- N/A

Configuration Steps

- Optional. You can enable the AP priority function according to requirements and configure the priority of a specified AP.
- On the AC device, enter the AC configuration mode and run the **ap-priority** { **enable** | **disable** } command to enable or disable the AP priority function.
- On the AC device, enter the AP configuration mode and run the **priority** *priority-value* command to configure the priority of a specified AP.

Command	**ap-priority** { **enable** | **disable**}
Parameter Description	**enable**: enables the AP to support the failover priority. **disable**: disables the AP to support the failover priority.
Defaults	Disable
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**priority** *priority-value*
Parameter Description	priority-value: indicates the AP priority. The value ranges from 1 to 4, where 1 is the lowest priority.
Defaults	The default priority of an AP is 1. The priority can be set to a value from 1 to 4, where 1 is the lowest priority and 4 is the highest priority. You can run the **priority** command in AP configuration mode to configure the AP priority.
Command Mode	AP configuration mode
Usage Guide	N/A

Verification

- Run the **show running** or **show ap-config running** command to check the configurations.

Configuration Example

Setting the Priority of FS-AP1 to 2 and Enabling the AP Priority Function

Configuration Steps	• Enter the AP configuration mode. • Configure the AP priority. • Enter the AC configuration mode.

	● Enable the AP priority function.
AC	FS(config)#ap-config FS-AP1 FS(config-ap)#priority 2 FS(config)#ac-controller FS(config-ac)#ap-priority enable
Verification	Run the **show running** command to check whether the **ap-priority enable** command is configured in AC configuration mode. Run the **show ap-config running** command to check the AP configurations.

AC	FS(config)#show running
	!
	ac-controller
	  ap-priority enable
	!
	FS#show ap-config running
	!
	ap-config FS-AP1
	  priority 2
	!

Common Errors

- N/A

1.4.19 Creating a WLAN

Configuration Effect

- You can create multiple WLANs on an AC and enter the configuration mode of a specified WLAN to configure related functions and properties of the WLAN according to the actual network requirements.
- The WLAN service template that is generated based on the following configurations can take effect only after the WLAN is deployed on a specified AP group. Wireless users can access related APs to access the WLAN.
- On the wireless network, you can divide the network into multiple WLAN subnets by creating WLANs. In addition, you can configure the functions and properties of a specified WLAN in WLAN configuration mode to provide different network services for wireless users.
- When creating a WLAN, you must associate the WLAN with an SSID, which is the name of a network service zone. One SSID can be mapped to one or multiple WLANs.

Notes

- N/A

Configuration Steps

- Optional. No WLAN is configured by default. You must create a WLAN before deploying the WLAN.
- Run the **wlan-config** command to create a WLAN, and use the **no** form of the command to delete the WLAN.

Command	**wlan-config** *wlan-id* [*profile –string*][*ssid-string*] **no wlan-config** *wlan-id*
Parameter Description	*wlan-id*: indicates the ID of a WLAN. The value ranges from 1 to 4094. *profile -string*: indicates the profile of the WLAN. This parameter is optional. The maximum length is 32 bytes. *ssid-string*: indicates the SSID. The maximum length is 32 bytes. When creating a WLAN, you must specify the SSID associated with the WLAN. Use the **no** form of the command to delete a specified WLAN.
Defaults	No WLAN is created by default.
Command Mode	Global configuration mode
Usage Guide	One SSID can be mapped to one or multiple WLANs, but one WLAN can be associated with only one SSID.

Verification

- Run the **show running** command to check the WLAN configurations.

Configuration Example

Creating a WLAN

Configuration Steps	• Create WLAN 1. The SSID of WLAN 1 is FS-wireless.
AC	FS(config)#wlan-config 1 FS-wireless FS(config-wlan)#
Verification	Run the **show running** command to check the WLAN configurations.
AC	FS#show running ! wlan-config 1 FS-wireless !

Common Errors

- N/A

1.4.20 Deploying a WLAN

Configuration Effect

- The WLAN configuration takes effect only after the WLAN is deployed on a specified AP group. Wireless users can access the WLAN through the related APs. Run the **interface-mapping** command in AP group configuration mode to deploy the WLAN on a specified AP group. This command also configures the mapping between the WLAN and the VLANs or VLAN group of the wired network.

Notes

- Assume that the WLAN forwarding mode is local forwarding. In this case, if the vlan-id assigned to a STA in vlan-id or vlan-group mode configured by this **interface-mapping** command is the same as the vlan-id specified by the **ap-vlan** command, the real VLAN of the STA will be determined by the access switch of the AP, instead of the VLAN configured by the **interface-mapping** command or the VLAN assigned in vlan-group mode. In particular, the default vlan-id of the ap-vlan is 1. If the ap-vlan is not configured and the vlan-id configured in the **interface-mapping** command is 1, the VLAN of the STA in local forwarding mode is determined by the access switch.

Configuration Steps

- Optional. You can run the **interface-mapping** command in AP group configuration mode to configure a WLAN and deploy the WLAN on all APs in the AP group.
- On the AC device, enter the AP configuration mode and run the **interface-mapping** command for configuration.

Command	**interface-mapping** *wlan-id*{*vlan-id* | **group** *vlan-group-id*}[**radio**{*radio-id* | [*802.11b* | *802.11a*]}] [**ap-wlan-id** *ap-wlan-id*]
Parameter Description	*wlan-id*: indicates the ID of the specified WLAN. This WLAN must have been created. The WLAN ID ranges from 1 to 4094. *vlan-id*: indicates the ID of the specified VLAN. The VLAN ID ranges from 1 to 4094. vlan-group-id: indicates the ID of the specified VLAN group. The VLAN group ID ranges from 1 to 128. r*adio-id*: indicates the ID of the radio of a specified AP. If radio-id is not specified, the mapping is applied to all radios of all APs in the AP group. *802.11b*: indicates that the mapping is applied to all 2.4 GHz radios of all APs in the AP group. *802.11a*: indicates that the mapping is applied to all 5.8 GHz radios of all APs in the AP group. *ap-wlan-id*: specifies the wlan-id that is used on the AP through interface-mapping. The value ranges from 1 to 64.
Defaults	By default, the WLAN is not deployed on any AP.
Command Mode	AP group configuration mode
Usage Guide	If the **ap-wlan-id** parameter is not specified, the mapping automatically selects and uses an idle ap-wlan-id.

Verification

- Run the **show running** command to check the AP group configurations.

Configuration Example

Configuring a WLAN and Deploying the WLAN on a Specified AP Group

Configuration Steps	FS-AP1 belongs to the AP group APG-1. Create a WLAN, and deploy the WLAN on FS-AP1. - Create WLAN 1. The SSID of WLAN 1 is FS-wireless. - Create VLAN 1. - Configure the WLAN-VLAN mapping in AP group configuration mode.
AC	FS(config)#wlan-config 1 FS-wireless FS(config-wlan)#exit FS(config)#vlan 1 FS(config-vlan)#exit

	FS(config)#ap-group APG-1 FS(config-ap-group)#interface-mapping 1 1
Verification	Run the **show running** command to check the AP group configurations.
	FS#show running ! wlan-config 1 FS-wireless ! ! ap-group APG-1 interface-mapping 1 1 !

Common Errors

- N/A

1.4.21 Enabling or Disabling WLAN SSID Broadcasting

Configuration Effect

- On the WLAN, the AP periodically broadcasts the SSID information to notify other entities of the existence of the wireless network. Wireless users use the wireless network interface cards (NICs) to search SSIDs and detect the wireless network. The SSID broadcasting function can be enabled to prevent the wireless network from being searched and connected by unauthorized users based on the SSID.

Notes

- N/A

Configuration Steps

- Optional. WLAN SSID broadcasting is enabled by default. If the WLAN SSID should be hidden to prevent the wireless network from being searched and connected by unauthorized users based on the SSID, you can disable the WLAN SSID broadcasting function.
- On the AC device, enter the WLAN configuration mode and run the **enable-broad-ssid** command for configuration.

Command	**enable-broad-ssid** **no enable-broad-ssid**
Parameter Description	N/A
Defaults	WLAN SSID broadcasting is enabled by default.
Command Mode	WLAN configuration mode
Usage Guide	WLAN SSID broadcasting is enabled by default. You can use the **no** form of the command to disable this function. If the SSID broadcasting configuration of the WLAN changes, users associated with the WLAN will go offline.

Verification

- Run the **show running** command to check the WLAN configurations.

Configuration Example

Disabling SSID Broadcasting of WLAN 1

Configuration Steps	● Enter the WLAN configuration mode. ● Disable SSID broadcasting.
AC	FS(config)#wlan-config 1 FS(config-wlan)#no enable-broad-ssid
Verification	Run the **show running** command to check the WLAN configurations.
AC	FS#show running ! wlan-config 1 FS-wireless no enable-broad-ssid !

Common Errors

- N/A

1.4.22 Configuring the NAS ID of a WLAN User

Configuration Effect

- On the WLAN, the NAS IDs of WLAN users identify different hot spot areas. By default, the NAS ID of a WLAN user is a null string.

Notes

- N/A

Configuration Steps

- Optional.
- On the AC device, enter the WLAN configuration mode and run the **nas-id** command to configure the NAS ID.

Command	**nas-id** *wlan-nas-id* **no nas-id**
Parameter Description	N/A
Defaults	Null string
Command Mode	WLAN configuration mode
Usage Guide	N/A

Verification

- Run the **show running** command to check the WLAN configurations.

Configuration Example

Configuring the NAS ID of a WLAN User

Configuration Steps	• Enter the WLAN configuration mode. • Configure the NAS ID of a WLAN user.
AC	FS(config)#wlan-config 1 FS(config-wlan)#nas-id0000059159100460
Verification	Run the **show running** command to check the WLAN configurations.
AC	FS#show running ! wlan-config 1 FS-wireless nas-id0000059159100460 !

Common Errors

- N/A
-

1.4.23 Configuring the WLAN SSID

Configuration Effect

- Configure a new SSID for the WLAN. If this WLAN has been deployed, all users associated with this WLAN will go offline.
- Configure the coded character set for the SSID. If the WLAN is deployed, all users of this WLAN will go offline.

Notes

- N/A

Configuration Steps

- Optional.
- On the AC device, enter the WLAN configuration mode and run the **ssid** command to configure the new SSID.

Command	**ssid** *ssid-string*
Parameter Description	N/A
Defaults	N/A
Command Mode	WLAN configuration mode
Usage Guide	N/A

- On the AC device, enter the WLAN configuration mode and run the **ssid-code** command to configure the coded character set for the SSID.

Command	**ssid-code** { **gbk** | **utf-8** }
Parameter Description	**gbk**: Configures gbk. **utf-8**: Configures utf-8.
Defaults	N/A
Command Mode	WLAN configuration mode
Usage Guide	If the WLAN is deployed, all users of this WLAN will go offline.

Verification

- Run the **show running** command to check the WLAN configurations.

Configuration Example

Configuring a New SSID "FS" for WLAN 1

Configuration Steps	• Enter the WLAN configuration mode. • Configure a new SSID "FS".
AC	FS(config)#wlan-config 1 FS(config-wlan)#ssid FS
Verification	Run the **show running** command to check the WLAN configurations.
AC	FS#show running ! wlan-config 1 FS !

Common Errors

- N/A

1.4.24 Configuring the AP Backup Function

Configuration Effect

- If the active AP in an AP backup group is faulty and disconnected, other standby APs in the group receive the WLAN configuration of the active AP and transmit radio signals of the active AP.

Notes

- In an AP backup group, if the active AP is not selected, the AP backup function does not take effect.

Configuration Steps

Configuring an AP Backup Group

- Optional. Create an AP backup group when the wireless network of an AP needs to be backed up.

- In AC configuration mode, run the **ap-backup group** command to create an AP backup group.

Command	**ap-backup group** *backup-group*
Parameter Description	*backup-group*: indicates the name of the AP backup group.
Defaults	By default, if only the AP backup group named "default" exists on the AC, the backup function of this group does not take effect.
Command Mode	AC configuration mode
Usage Guide	N/A

Adding APs to an AP Backup Group

- Optional. When the wireless network of an AP must be backed up by other APs, add the standby APs and the AP to be backed up to the AP backup group, and select the AP to be backed up as the active AP.

- In AP configuration mode, run the **ap-backup-group** command to add the AP to the AP backup group. When adding an AP to an AP backup group, you can specify whether the AP is the active AP.

Command	**ap-backup-group** *backup-group***[master]**
Parameter Description	*backup-group*: indicates the name of the AP backup group.
Defaults	By default, the AP is not added to the default group, and the backup function of the backup group does not take effect.
Command Mode	AP configuration mode
Usage Guide	This command does not support the ap-config all mode. The keyword **master** is optional. If the command contains this keyword, the AP is designated as the active AP of the group; otherwise, the AP is the standby AP. An AP backup group can have multiple standby APs but only one active AP. When the AP backup group starts to work, that is, the standby APs have inherited WLAN signals from the active AP, note that the following four operations change the WLAN configurations of the standby APs that should take effect, and the inherited WLAN signals will take effect again: 1. Modify the WLAN configurations of the AP group to which the standby APs belong. 2. Modify the WLAN configurations of the AP group to which the active AP belongs. 3. Change the AP group of the standby APs. 4. Change the AP group of the active AP. If online users already exist, these users will go offline.

Verification

- Run the **show ap-config running** and **show ac-config ap-backup-group** commands to check the configurations.

Configuration Example

Creating an AP Backup Group Named "APBACK-APG-1"

Configuration Steps	● In AC configuration mode, run the **ap-backup group** command to create an AP backup group.
AC	FS(ac-config)#ap-backup group APBACK-APG-1
Verification	● Run the **show ac-config ap-backup-group** command to check the configurations.
AC	FS#show ac-config ap-backup-group Cnt Group-Name Master-AP cnt Standby-AP cnt Master-AP-Name Working ------ ---------- ---------- ---------- ---------- 1 APBACK-APG-1 1 2 AP4210-1 false

Adding ap4210-1 to the AP Backup Group Named "APBACK-APG-1", and Configuring this AP as the Active AP of the Group

Configuration Steps	● In AP configuration mode, run the **backup-group** command to add the AP to the AP backup group.
AC	FS(ap-config)#ap-backup-group APBACK-APG-1 master
Verification	● Run the **show ac-config ap-backup-group** command to check the configurations.
AC	FS#show ac-config ap-backup-groupAPBACK-APG-1 Cnt Ap-Name Ap-Mac Online Is-Master Inherit-Wlan Cnt ------- ---------- ---------- ------- ---------- ---------- 1 AP4210-1 8832.0000.1111 true Yes 0

Common Errors

● N/A

1.5 Monitoring

Displaying

Description	Command
Displays the basic configurations of the current AC	**show ac-config**
Displays the AP backup group information	**show ac-config ap-backup-group**
Displays the BSSID list of all APs	**show ap-config bssid**
Displays the AP status information	**show ap-config cb**
Displays the WLAN information inherited by the AP	**show ap-config inherit-wlan**
Displays the AP product list	**show ap-config product**
Displays the current status of all APs	**show ap-config summary**
Displays authentication-related information of all APs	**show ap-config summary ap-auth**
Displays APs that try to associate with the AC but are rejected by the AC	**show ap-config summary deny-ap**

Description	Command
Displays the APs in a specified AP group	**show ap-group aps**
Displays the APs in all AP groups	**show ap-group aps summary**
Displays the basic information about a specified AP	**show ap-group cb**
To display the WLAN-VLAN mapping of a specified AP group	**show ap-group intf-wlan-map**
Displays all APs	**show ap-group summary**
Displays the basic information about a specified WLAN	**show wlan-config cb**
Displays the WLAN configuration list on the AC	**show wlan-config summary**

2 Configuring STA Management

2.1 Overview

STA Management (STAMG) implements station (STA) management, including STA access control management and STA event notification. Event notification is mainly used to serve other function modules. Applications of the STAMG functions are as follows:

- The dynamic blacklist is used on a security-sensitive network to prevent user attacks.
- The STA limit is used when the number of STAs exceeds the AP capacity.
- Load balancing is used when STAs need to be evenly distributed to multiple APs.
- Association control is used in the E-bag scenario.

Protocols and Standards

- N/A

2.2 Applications

Application	Description
Fit AP Networking	In fit AP network mode, at least one AC and one AP are required.
Large Conference Room	In fit AP network mode, at least one AC and two APs are required.
E-Bag	In fit AP network mode, at least one AC and two APs are required.

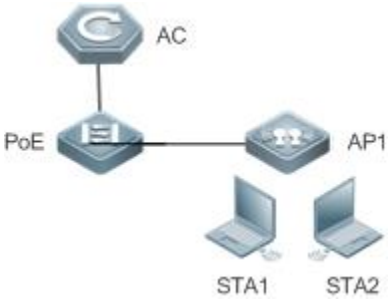
2.2.1 Fit AP Networking

Scenario

One AC is deployed on the wireless network, and dynamic blacklist and STA limit functions are enabled on the AC.

As shown in Figure 2-1, dynamic blacklist and STA limit are enabled on the AC.

Figure 2-1



Remarks	AC is the wireless access controller. PoE is the switch that functions as the gateway of APs. AP is the wireless access device. STA1 and STA2 are user devices.

Deployment

- Enable dynamic blacklist and STA limit on the AC.

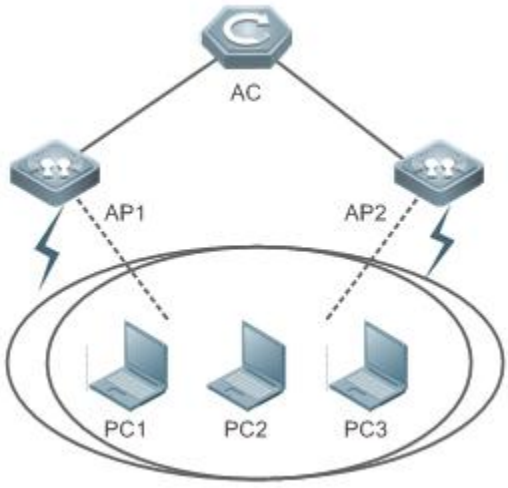
2.2.2 Large Conference Room

Scenario

In a large conference room, the number of STAs is generally large, and STAs must be evenly distributed to multiple APs; otherwise, too many STAs are connected to some specific APs, resulting in a low network speed and a poor user experience.

As shown in Figure 2-2, two APs (AP1 and AP2) are deployed in the conference room so that STAs can be evenly distributed to the two APs.

Figure 2-2



Remarks	AC is the wireless access controller. AP1 and AP2 are wireless access devices. PC1, PC2, and PC3 are user devices.

Deployment

- Enable load balancing on the AC, and add AP1 and AP2 to the load balancing group.

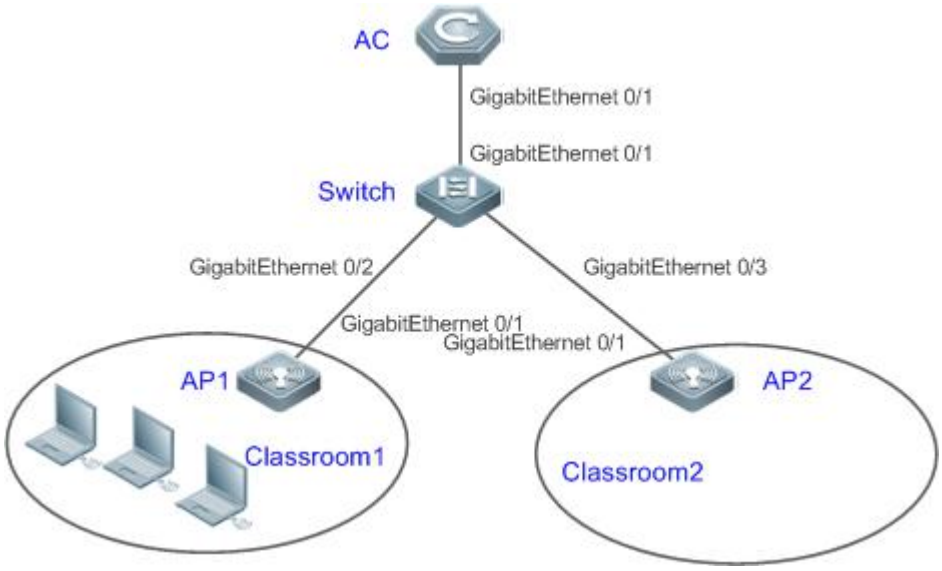
2.2.3 E-Bag

Scenario

One AC is deployed on the wireless network, and multiple APs are deployed in different classrooms. When the teacher's STA is associated with an AP, the students' STAs must also be associated with the same AP. This ensures the network transmission speed.

As shown in Figure 2-3, AP1 is deployed in Classroom1 and AP2 is deployed in Classroom2. When the teacher's STA is associated with AP1, the students' STAs must also be associated with AP1, instead of AP2. In this way, traffic destined for Classroom1 is only sent to AP1 without affecting users on AP2.

Figure 2-3



Remarks	AC is the wireless access controller. Switch functions as the gateway of APs. AP1 and AP2 are wireless access devices.

In the E-bag scenario, if the teacher uses the wired network connection, one of STAs used by students must be configured as the primary STA to implement association control. Who uses this primary STA is determined by users themselves. For example, the primary STA can be used by the class monitor or the teacher so that secondary STAs can be associated correctly. After correct association of the secondary STAs, the teacher can put this primary STA aside, and use the wired network connection during the class.

Deployment

- Enable association control on the AC, and add APs to a specified association control zone.

2.3 Features

Overview

Feature	Description
Dynamic Blacklist	Detects association of unauthorized users.
STALimit	Limits the number of STAs.
Load Balancing	Distributes STAs evenly to multiple APs.
Inter-Radio Load Balancing	Distributes STAs evenly to multiple radios of the same AP.
Association Control	Associates secondary STAs with APs in the same control zone if the primary STA is associated with these APs.
STA Management	Disassociates STAs without traffic forcibly to recycle resources.
STA Informational Syslog Suppression	Suppresses the informational syslog output rate of STAs.

2.3.1 Dynamic Blacklist

The AC can use the dynamic blacklist to punish malicious or unauthorized STAs so that these STAs cannot be associated within a period of time. In addition, the dynamic blacklist can be used to disassociate these STAs.

Working Principle

The number of STA association failures (including failures caused by incorrect user names or passwords) is counted in a period of time. When the number of association failures of an STA exceeds a certain threshold, the STA is added to the blacklist. STAs in the blacklist cannot be associated within a period of time.

2.3.2 STA Limit

STA limit aims to limit the number of STAs that can be associated with an AP based on the load capacity. This prevents the risk of insufficient resources caused by overload of APs.

Working Principle

When STAs are associated, the AP checks whether the number of associated STAs exceeds the threshold. If yes, STAs cannot be associated.

2.3.3 Load Balancing

Load balancing can balance the load among APs managed by an AC. The load here can be traffic or the number of associated STAs. The purpose is to prevent the problem that some APs are overloaded and some APs are in the idle state.

Working Principle

When an STA tries to be associated, if the load on the AP associated by the STA exceeds the preset threshold, the system checks whether the load difference between all the APs in the load balancing group of this AP exceeds the threshold. If yes, the STA is not allowed to associate with this AP. The load difference can be configured as the number of STAs or the traffic.

To prevent the problem that the STA can receive signals from only one AP but fails to be associated due to load balancing, the maximum number of load balancing times can be configured. If association fails for consecutively twice due to load balancing, load balancing is not performed for the third time and the STA can be associated with the AP.

2.3.4 Inter-Radio Load Balancing

Inter-radio load balancing can balance the load among radios of the same AP to prevent overload of a single radio. Similarly, the load here can be the traffic or the number of associated STAs.

Working Principle

The principle of inter-radio load balancing is similar to that of load balancing group except that you can configure the load balancing thresholds respectively for intra-radios (2.4 GHz or 5 GHz) or inter- radios. If the AP has both 2.4 GHz or 5 GHz radio, intra- radio settings take effect. Otherwise, inter-radio settings take effect.

2.3.5 Association Control

Association control is a method for controlling association behaviors of wireless STAs. STAs are divided into two groups. In each group, only one STA is defined as the primary STA, and the other STAs are defined as secondary STAs. The secondary STAs must follow the association behaviors of the primary STA. That is, the primary and secondary STAs must be associated with the same wireless network. In this way, association behaviors of wireless STAs can be properly controlled.

Working Principle

The coverage area of a wireless network is divided into several association control zones. One or several APs are deployed in each zone, and wireless terminals are divided into groups. The control zones that can be associated with the terminals are strictly controlled. For example, a school has many classrooms, and a wireless AP is deployed in each classroom. Radio signals travel in the space. When E-bags are used in two adjacent classrooms at the same time, the ideal condition is that all the teacher and student terminals are associated with

the AP of their own classrooms so that the two classrooms will not interfere with each other. In this case, a classroom must be defined as an association control zone and all the teacher and student terminals in a classroom must be associated with the AP of the classroom.

Association control aims to prevent terminals from associating with a wireless network at random when multiple wireless networks are available for selection. The following are prerequisites for network configurations:

- Based on the pre-configured association control zones and package information, the AC pushes the information about primary STAs in all packages to all APs in the association control zones and generates a whitelist of primary STAs on these APs.
- The information about primary STAs in all packages is available in the AP whitelist. Therefore, before the association control function is enabled, the primary STA must associate itself with the corresponding SSID in the specified control zone. After that, the AC pushes all corresponding secondary STAs to all APs in the association control zone and generates a whitelist according to the configuration of the primary STA package to allow the secondary STAs to associate themselves with the control zone.
- When the primary STA is de-associated from the control zone, all the secondary STAs will also be de-associated and deleted from the AP whitelist.
- The above process can be summarized as follows: The secondary STAs must follow the primary STA to associate themselves with an AP in the same control zone, with which the primary STA is associated. Only the APs of this control zone have a whitelist of the corresponding secondary STAs. This ensures that STAs are not randomly associated with APs.

2.3.6 STA Management

STA management is used to manage association and disassociation logic processing of STAs.

Working Principle

In normal cases, an STA sends a disassociation frame to inform the AC that the STA is disassociated. If the STA does not send a disassociation frame to the AC when it is disassociated abnormally (for example, because the user removes the network interface card (NIC)), the AC cannot learn the disassociation of the STA. In this case, the AC detects the STA traffic and finds that the STA has no traffic within a period of time, and concludes that the STA had been disassociated. Then, the AC performs disassociation processing on the STA.

2.3.7 STA Informational Syslog Suppression

STA informational syslog suppression prevents a high CPU usage caused by the large number of informational syslogs generated when STAs are frequently associated or disassociated.

Working Principle

The number of syslogs output per second is counted. When this number reaches the upper limit, no more syslog is output within the second, thereby suppressing the syslog. In the next second, the number of syslogs is counted again.

2.4 Configuration

Configuration	Description and Command	
Configuring Dynamic Blacklist	(Mandatory) It is used to enable the dynamic blacklist function.	
	sta-blacklist enable	Enables the dynamic blacklist function.
	(Optional) It is used to configure the parameters of the dynamic blacklist.	
	sta-blacklist lifetime	Configures the lifetime of the dynamic blacklist.

	sta-blacklist detect-time	Configures the detection time of the dynamic blacklist.
	sta-blacklist fail-limit	Configures the maximum number of association failures.
Configuring STA Limit	(Optional) It is used to configure the maximum number of STAs.	
	sta-limit	Configures the maximum number of STAs.
	sta-limit radio	Configures the maximum number of STAs that can be associated with a radio of the AP.
Configuring Load Balancing	(Mandatory) It is used to configure load balancing.	
	num-balance-group create	Creates a number-based balancing group.
	num-balance-group add	Adds an AP to the number-based balancing group.
	num-balance-group del	Deletes an AP from the number-based balancing group.
	flow-balance-group create	Creates a traffic-based balancing group.
	flow-balance-group add	Adds an AP to the traffic-based balancing group.
	flow-balance-group del	Deletes an AP from the traffic-based balancing group.
	(Optional) It is used to configure the load balancing parameters.	
	num-balance-group num	Configures the threshold of the number-based balancing group.
	num-balance-group mode	Configures the working mode of the number-based balancing group.
	flow-balance-group flow	Configures the threshold of the traffic-based balancing group.
	flow-balance-group radio-flow	Enables a specified traffic balancing group to use the traffic uploaded by APs.
Configuring Inter-Radio Load Balancing	(Mandatory) It is used to enable the load balancing function among radios.	
	inter-radio-balance flow-balance enable	Enables inter-radio traffic-based balancing.
	inter-radio-balance num-balance enable	Enables inter-radio number –based balancing.
	(Optional) It is used to configure the load balancing parameters.	
	inter-radio-balance flow-balance dual-band	Configures parameters for traffic –based balancing among inter-frequency radios.
	inter-radio-balance flow-balance same-band	Configures parameters for traffic –based balancing among intra-frequency radios.
	inter-radio-balance num-balance dual-band	Configures parameters for number-based balancing among inter-frequency radios.

	inter-radio-balance num-balance same-band	Configures parameters for number-based balancing among intra-frequency radios.
Configuring Association Control	(Mandatory) It is used to enable the association control function.	
	package	Configures a package.
	primary-sta	Configures the primary STA in the package.
	secondary-sta	Configures the secondary STA in the package.
	control-zone	Configures an association control zone.
	ap	Configures the AP information.
	assoc-control	Enables association control.
Configuring STA Management	(Optional) It is used to configure the time after which the STA is disassociated if no traffic is detected.	
	sta-idle-timeout	Configures the time after which the STA is disassociated if no traffic is detected.
Configuring STA Informational Syslog Suppression	(Optional) It is used to configure the maximum output rate of the STA informational syslogs.	
	sta-logging rate-limit	Configures the maximum output rate of the STA informational syslogs.

2.4.1 Configuring Dynamic Blacklist

Configuration Effect

- When it is detected that the number of association failures on an STA reaches the threshold within the specified time, this STA is added to the blacklist.

Notes

- The time period is not fixed and is between **detect-time** and (**detect-time** + 5).**detect-time** is expressed in second. This factor must be considered during configuration.
- If multiple authentication modes are applied, the number of STA association failures increases by 1 so far as one of the authentication modes fails. Combinations of authentication modes include, but are not limited to, PSK+Web, PSK+MAB+Web, PSK+MAB, MAB+Web, and 802.1x+Web.

Configuration Steps

Enabling Dynamic Blacklist

- (Mandatory) Enable the dynamic blacklist function on an AC or a fat AP.

Command	**sta-blacklist enable**
Parameter Description	N/A
Defaults	The blacklist function is disabled.
Command Mode	AC configuration mode
Usage Guide	N/A

Configuring the Dynamic Blacklist Parameters

- (Optional) Configure the dynamic blacklist parameters on an AC or a fat AP.
- Configure the blacklist lifetime.
- Run the **sta-blacklist lifetime** command to configure the lifetime of the dynamic blacklist. A longer lifetime indicates a longer period of time within which the STA added to the blacklist is not allowed to associate itself with the AC.
- Run the **sta-blacklist detect-time** command to configure the detection time. As the detection time decreases, the unauthorized STA detection becomes more sensitive and the number of false reports increases.
- Run the **sta-blacklist fail-limit** command to configure the upper limit of association failures. A larger upper limit indicates that an STA can make more association attempts.

Command	**sta-blacklist lifetime** *seconds*
Parameter Description	*seconds:* Indicates the blacklist lifetime. The value ranges from 60s to 1200s.
Defaults	300s
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**sta-blacklist detect-time** *seconds*
Parameter Description	*seconds:* Indicates the STA detection time. The value ranges from 5s to 60s.
Defaults	60s
Command Mode	AC configuration mode
Usage Guide	This command is used to configure the STA detection time. When encountering the first association failure, the STA is listed as a suspected attacker. If the number of association failures on the STA reaches the upper limit (namely, the **fail-limit**) within the detection time, the STA is added to the blacklist.

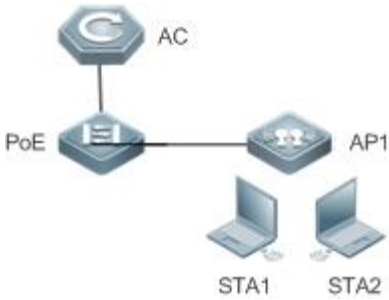
Command	**sta-blacklist fail-limit** *number*
Parameter Description	*number*: Indicates the maximum number of association failures. The value ranges from 1 to 100.
Defaults	5
Command Mode	AC configuration mode
Usage Guide	N/A

Verification

- Run the **show sta-blacklist** command to display the STAs in the blacklist.

Configuration Example

Configuring Dynamic Blacklist

Scenario Figure 2-4	
Configuration Steps	● Configure the dynamic blacklist function.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# ac-controller AC(config-ac)# sta-blacklist enable
Verification	● After the CAPWAP tunnel is established between an AP and an AC, enter an incorrect password for several times to verify that the STA can be added to the blacklist.
AC	AC# show sta-blacklist Num STA MAC Add time ---------- ---------- ---------- 1 0080.1111.1111 2013-07-02 13:56:22 2 0090.2222.3333 2013-07-02 13:56:35 3 0070.1111.2233 2013-07-02 13:57:08

Common Errors

- N/A

2.4.2 Configuring STA Limit

Configuration Effect

- Limit the maximum number of STAs that can be associated with an AC, a WLAN, an AP, or a radio of an AP on the wireless network.

Notes

- The STA limits configured for an AC, a WLAN, an AP, or a radio of an AP take effect simultaneously. That is, an STA can be associated only if all the STA limits are met.
- The STA limit configured on the AC is subject to the license.

Configuration Steps

Configuring STA Limit

- (Optional) Configure the STA limitation an AC or a fat AP.
- If the number of STAs on the wireless network is large, the STA limit can be configured to allow more STAs are associated, but the total bandwidth will decrease.
- Run the **sta-limit** command to configure the STA limit. A large STA limit indicates that more STAs can be associated.
- The AC-based STA limit is (32 x Number of APs) by default. The WLAN-based STA limit is not specified by default. The AP-based STA limit is 32 by default.
- Run the **sta-limit radio** command to configure the radio-based STA limit for an AP. A large STA limit indicates that more STAs can be associated.
- Run the **sta-limit per-ap** command to configure the maximum number of STAs supported on each AP in a WLAN. By default, the number of STAs on an AP is not limited. If the number of configured STAs exceeds the maximum number of STAs supported by an AP, no new STA can associate with the AP.

Command	**sta-limit** *max-num*
Parameter Description	*max-num*: Indicates the maximum number of STAs. The value varies according to the configuration mode and device.
Defaults	In AC configuration mode, the default value is (32 x Number of APs supported by the AC), depending on the license. In AP group configuration mode, the default value is 32. In AP configuration mode, the default value is 32 for a disassociated AP or in the **ap-config all** configuration mode. The default value for an associated AP is determined by the AP model. In WLAN configuration mode, the STA limit is not specified.
Command Mode	AC configuration mode, WLAN configuration mode, AP configuration mode, or AP group configuration mode
Usage Guide	If the maximum number of STAs configured for a disassociated AP exceeds the actual capacity, the STA limit automatically changes to the actual maximum number of STAs supported after the AP is associated.

Command	**sta-limit** *max-num* **radio** *radio-id*
Parameter Description	*max-num*: Indicates the maximum number of STAs. The value ranges from 1 to 156. *radio-id*: Indicates the radio ID. The value ranges from 1 to 32.
Defaults	The STA limit is not specified by default.
Command Mode	AP configuration mode AP group configuration mode
Usage Guide	If the maximum number of STAs configured for a disassociated AP exceeds the actual capacity of the radio, the STA limit automatically changes to the actual maximum number of STAs supported after the AP is associated.

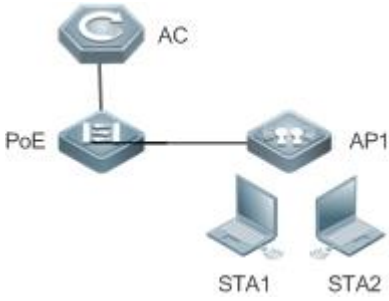
Command	**sta-limit per-ap** *max-num*
Parameter Description	*max-num*: Indicates the maximum number of STAs supported on an AP. The value ranges from 1 to 1536.
Defaults	By default, the number of STAs supported on an AP is not limited.
Command Mode	WLAN configuration mode
Usage Guide	N/A

Verification

- Verify that the number of STAs is limited.

Configuration Example

Configuring STA Limit

Scenario **Figure 2-5**	
Configuration Steps	● Configure the STA limit.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# ap-config ap1 AC(config-ap)# sta-limit64
Verification	● After the CAPWAP tunnel is established between an AP and an AC, check the AC running configuration.
AC	AC# show ap-config running ap-config ap1 sta-limit 64 !

Common Errors

- N/A

2.4.3 Configuring Load Balancing

Configuration Effect

- Enable even distribution of STAs on multiple APs in a load balancing group.

Notes

- Load balancing is applicable only to STAs that are associated, but not to STAs that are disassociated. Therefore, after STAs are disassociated, the traffic difference between APs or the STA quantity difference may exceed the threshold.

- Load balancing takes effect only on the same type of radios (2.4 GHz or 5 GHz). If the types of radios are different, load balancing is performed only when the AP reports that the STAs are capable of dual-band operation. Otherwise, the 2.4 GHz STAs may fail to be associated with 2.4 GHz radios when no STA is associated with 5 GHz radio.
- After the traffic-based balancing group is configured to use the traffic information uploaded by APs, APs must upload the traffic information to the AC at a regular interval because the traffic only exists on APs and is not routed to the AC. During this interval, the traffic information on the AC does not change. At this time, if the traffic between APs is not balanced, STAs cannot be associated with APs with heavy traffic until the APs upload the traffic information to the AC.

Configuration Steps

Creating a Number-based Balancing Group

- (Mandatory)Create a number-based balancing group on the AC.
- APs can be only added to a created load balancing group.

Command	**num-balance-group create** *group-name*
Parameter Description	*group-name*: Indicates the name of a load balancing group.
Defaults	No number-based balancing group is created.
Command Mode	AC configuration mode
Usage Guide	N/A

Adding an AP to the Number-based Balancing Group

- (Mandatory) The configuration is performed on the AC.
- Load balancing applies to the APs which are added to the load balancing group.

Command	**num-balance-group add** *group-name ap-name*
Parameter Description	*group-name*: Indicates the name of a load balancing group. *ap-name*: Indicates the AP name.
Defaults	No AP is added to the number-based balancing group.
Command Mode	AC configuration mode
Usage Guide	N/A

Creating a Traffic-based Balancing Group

- (Mandatory) The configuration is performed on the AC.
- APs can be only added to a created load balancing group.

Command	**flow-balance-group create** *group-name*
Parameter Description	*group-name*: Indicates the name of a load balancing group.
Defaults	No traffic-based balancing group is created.
Command Mode	AC configuration mode
Usage Guide	N/A

Adding an AP to the Traffic-based Balancing Group

- (Mandatory) The configuration is performed on the AC.

- Load balancing applies to the APs which are added to the load balancing group.

Command	**flow-balance-group add** *group-name ap-name*
Parameter Description	*group-name*: Indicates the name of a load balancing group. *ap-name*: Indicates the AP name.
Defaults	No AP is added to the traffic-based balancing group.
Command Mode	AC configuration mode
Usage Guide	N/A

Configuring Parameters of Load Balancing Group

- (Optional) Configure the parameters of load balancing group on the AC.
- Run the **num-balance-group num** command to configure the threshold of number-based balancing group. A larger threshold indicates a greater difference in the number of STAs associated with two APs, and the less balanced load.
- Run the **num-balance-group mode** command to configure the radio-based balancing function. If radio-based balancing is enabled, the control on the distribution of STAs is more accurate, but the effect of balancing among APs is less satisfying.
- Run the **num-balance-group enable** command to configure the trigger threshold of the number-based balancing group. A higher trigger threshold indicates that load balancing is enabled only when the AP load is heavy.
- Run the **num-balance-group del** command to delete an AP from the number-based balancing group.
- Run the **flow-balance-group flow** command to configure the traffic-based balancing threshold. A higher traffic balancing threshold indicates that the traffic difference between two APs is greater and the traffic is less balanced.
- Run the **flow-balance-group radio-flow** command to enable the traffic balancing group to use the traffic information uploaded by APs. In local forwarding mode, data packets are not routed to the AC, and the AC cannot obtain the traffic information. Therefore, the traffic information uploaded by APs must be used to determine whether to enable load balancing.
- Run the **flow-balance-group enable** command to configure the trigger threshold of the traffic-based balancing group. A higher trigger threshold indicates that load balancing is enabled only when the AP load is heavy.
- Run the **flow-balance-group del** command to delete an AP from the traffic-based balancing group.
- Run the **flow-balance-group base** command to configure the baseline of traffic balancing in global configuration mode.
- Run the **sta-balance num-limit enable** command to limit the maximum times of load balancing.

Command	**num-balance-group num** *group-name number*
Parameter Description	group-name: Indicates the name of a load balancing group. number: Indicates the trigger threshold. The default value is 3. The value ranges from 0 to 20, where 0 indicates that the number balancing function is disabled for the load balancing group.
Defaults	3
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**num-balance-group mode** *group-name*{ **radio-mode**| **ap-mode** }
Parameter Description	*group-name:* Indicates the name of a load balancing group.
Default s	AP-based number balancing

Command Mode	AC configuration mode
Usage Guide	N/A

Command	**num-balance-group enable** *group-name number*
Parameter Description	*group-name:* Indicates the name of a load balancing group. *number*: indicates the trigger threshold. The default value is 3. The value ranges from 0 to 10, where 0 indicates that the number balancing function is disabled for the load balancing group.
Defaults	3
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**num-balance-group del** *group-name ap-name*
Parameter Description	*group-name*: Indicates the name of a load balancing group. *ap-name*: Indicates the AP name.
Defaults	N/A
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**flow-balance-group flow** *group-name number*
Parameter Description	*group-name:* Indicates the name of a load balancing group. *number*: indicates the trigger threshold. The unit is %. The default value is 5%. The value ranges from 0 to 1000, where 0 indicates that the load balancing function is disabled for the load balancing group. The percentage baseline is 10 Mbps by default.
Defaults	5%
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**flow-balance-group radio-flow** *group-name*
Parameter Description	*group-name:* Indicates the name of the traffic balancing group.
Defaults	Traffic information on the CAPWAP data channel is used on the AC.
Command Mode	AC configuration mode
Usage Guide	You can enable a traffic balancing group to use the traffic information uploaded by APs. In this way, the traffic balancing group can receive the traffic information periodically sent by APs for load balancing.

Command	**flow-balance-group enable** *group-name number*
Parameter Description	*group-name:* Indicates the name of a load balancing group. *number*: Indicates the trigger threshold. The unit is %. The default value is 5%. The value ranges from 0 to 500, where 0 indicates that the load balancing function is disabled for the load balancing group. The percentage baseline is 10 Mbps by default.

Defaults	5%
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**flow-balance-group del** *group-name ap-name*
Parameter Description	*group-name:* Indicates the name of a load balancing group. *ap-name:* Indicates the AP name.
Defaults	N/A
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**flow-balance-group base** *number*
Parameter Description	*number*: Indicates that traffic baseline. The default value is 10 Mbps. The value ranges from 1 to 100.
Defaults	10 Mbps
Command Mode	AC configuration mode
Usage Guide	N/A

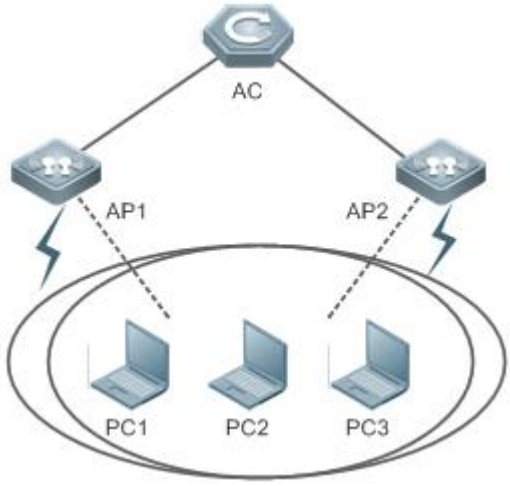
Command	**sta-balance num-limit enable**
Parameter Description	N/A
Defaults	The function is disabled by default.
Command Mode	AC configuration mode
Usage Guide	N/A

Verification

- Number balancing: Check whether the difference in the number of STAs associated with APs in the load balancing group is within the threshold.
- Traffic balancing: Check whether the difference in the traffic of APs in the load balancing group is within the threshold.

Configuration Example

Configuring Traffic Balancing

Scenario **Figure 2-6**	
Configuration Steps	● Create a load balancing group. ● Set the trigger threshold of this load balancing group to 1000 Kbps. ● Add AP1 and AP2 to the load balancing group named **test-group.** (If two APs are added to the same load balancing group, PCs in this group can search the RF signals of all APs.)
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)#ac-controller AC(config-ac)#flow-balance-group create test-group AC(config-ac)#flow-balance-group flow test-group 10 AC(config-ac)#flow-balance-group add test-group AP1 AC(config-ac)#flow-balance-group add test-group AP2
Verification	● Check the configuration of the load balancing group.
AC	AC# show ac-config flow-balance summary Group State Enable Threshold Base mode AP NAME ---------- ----- ---------- --------- ---- ---------- ---------- test-group UP 5*100kbps 10% 10 ap-mode(0) AP1, AP2

Common Errors

- N/A

2.4.4 Configuring Inter-Radio Load Balancing

Configuration Effect

- Enable inter-radio load balancing on APs to balance the load among radios.

Notes

- This function is not applicable to the i-Share solution. Signals of different radios cover different areas. An STA may receive signals from one or several radios. In this case, the inter-radio load balancing function cannot be enabled.
- Load balancing is applicable only to STAs that are associated. Therefore, after STAs are disassociated, the traffic difference between APs or the STA quantity difference may exceed the threshold.
- If the radio that an STA attempts to associate with is different from the radio with the lowest load, load balancing is performed only when the AP reports that the STA is capable of dual-band operation. Otherwise, the 2.4 GHz STAs may fail to be associated with 2.4 GHz radios when no STA is associated with 5 GHz radio.
- After the traffic balancing group is configured to use the traffic information uploaded by APs, APs must upload the traffic information to the AC at a regular interval because the traffic only exists on APs in local forwarding mode. During this interval, the traffic information on the AC does not change. At this time, if the traffic between APs is not balanced, STAs cannot be associated with APs with heavy traffic until the APs upload the traffic information to the AC.
- Configuration of load balancing parameters varies according to the inter-radio and intra-radio. If the AP has both 2.4 GHz or 5 GHz radio, intra- radio settings take effect. Otherwise, inter-radio settings take effect.
- When performing load balancing, determine the load balancing parameter according to the target radio and the type of the radio associated with the STA. Then, determine whether to associate the STA to the target radio. For a specific AP, so far as load balancing is enabled in any of the ap-config, ap-group, and ap-config all modes, load balancing is enabled on this AP. If the load balancing configurations in the three modes are different, the configurations take effect in the following sequence: ap-config > ap-group > ap-config all.
- When inter-radio load balancing is enabled, the association attempt of the same STA will be denied for at most twice within five minutes. If the STA is still associated with a radio with a heavy load for the third time, the association is allowed. Therefore, the effect of inter-radio load balancing is related to the actual STA behaviors.

Configuration Steps

Enabling Inter-radio Traffic Balancing

- (Mandatory). The configuration is performed on the AC. After the function is enabled, traffic is balanced whenever possible among different radios of the same AP.
- This function can be enabled for a single AP, all APs in an AP group, or all APs (configured in ap-config all mode).

Command	**inter-radio-balance flow-balance enable**
Parameter Description	N/A
Defaults	Inter-radio traffic balancing is disabled.
Command Mode	AP configuration mode, AP group configuration mode
Usage Guide	N/A

Enabling Inter-radio Number Balancing

- (Mandatory)The configuration is performed on the AC. After the function is enabled, the number of STAs is balanced whenever possible among different radios of the same AP.
- This function can be enabled for a single AP, all APs in an AP group, or all APs (configured in ap-config all mode).

Command	**inter-radio-balance num-balance enable**

Parameter Description	-
Defaults	Inter-radio number balancing is disabled.
Command Mode	AP configuration mode, AP group configuration mode
Usage Guide	N/A

Configuring Inter-radio Load Balancing Parameters

- (Optional) The configuration is performed on the AC. Parameters can be adjusted based on actual requirements of network optimization.
- Run the **inter-radio-balance flow-balance dual-band enable-load** *en-num* **threshold** *thrs-num* command to configure the trigger threshold and the load threshold for traffic balancing among inter-frequency radios. A smaller trigger threshold indicates that it is easier to enable load balancing. A smaller load threshold indicates that the load is better balanced.
- Run the **inter-radio-balance flow-balance same-band enable-load** *en-num* **threshold** *thrs-num* command to configure the trigger threshold and the load threshold for traffic balancing among intra-frequency radios. A smaller trigger threshold indicates that it is easier to enable load balancing. A smaller load threshold indicates that the load is better balanced.
- Run the **inter-radio-balance num-balance dual-band enable-load** *en-num* **threshold** *thrs-num* command to configure the trigger threshold and the load threshold for number balancing among inter-frequency radios. A smaller trigger threshold indicates that it is easier to enable load balancing. A smaller load threshold indicates that the load is better balanced.
- Run the **inter-radio-balance num-balance same-band enable-load** *en-num* **threshold** *thrs-num* command to configure the trigger threshold and the load threshold for number balancing among intra-frequency radios. A smaller trigger threshold indicates that it is easier to enable load balancing. A smaller load threshold indicates that the load is better balanced.

Command	**inter-radio-balance flow-balance dual-band enable-load** *en-num* **threshold** *thrs-num*
Parameter Description	en-num: Indicates the trigger threshold. The unit is 100 kbps. The value ranges from 1 to 1000. thrs-num: Indicates the load threshold. The unit is 100 Kbps. The value ranges from 1 to 1000.
Defaults	By default, both the trigger threshold and the load threshold are 10.
Command Mode	AP configuration mode, AP group configuration mode
Usage Guide	N/A

Command	**inter-radio-balance flow-balance same-band enable-load***e n-num* **threshold** *thrs-num*
Parameter Description	en-num: Indicates the trigger threshold. The unit is 100 kbps. The value ranges from 1 to 1000. thrs-num: Indicates the load threshold. The unit is 100 Kbps. The value ranges from 1 to 1000.
Defaults	By default, both the trigger threshold and the load threshold are 5.
Command Mode	AP configuration mode, AP group configuration mode
Usage Guide	N/A

Command	**inter-radio-balance num-balance dual-band enable-load** *en-num* **threshold** *thrs-num*
Parameter Description	en-num: Indicates the trigger threshold. The value ranges from 1 to100. thrs-num: Indicates the load threshold. The value ranges from 1 to 100.
Defaults	By default, both the trigger threshold and the load threshold are 8.
Command Mode	AP configuration mode, AP group configuration mode
Usage Guide	N/A

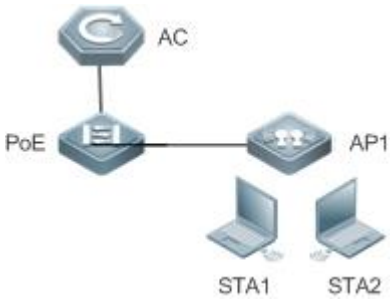
Command	**inter-radio-balance num-balance same-band enable-load** *en-num* **threshold** *thrs-num*
Parameter Description	en-num: Indicates the trigger threshold. The value ranges from 1 to 100. thrs-num: Indicates the load threshold. The value ranges from 1 to 100.
Defaults	By default, both the trigger threshold and the load threshold are 10 respectively.
Command Mode	AP configuration mode, AP group configuration mode
Usage Guide	N/A

Verification

- Number balancing: Run the **show ap-config summary** command to check whether the difference in the number of STAs between radios of the AP where load balancing is within the threshold.
- Traffic balancing: Run the **show ac-config client** command to check whether the traffic difference between radios of the AP where load balancing is enabled is within the threshold.

Configuration Example

Enabling Inter-radio Number Balancing on All APs in the Default AP Group

Scenario **Figure 2-7**	
Configuration Steps	● Enter the default AP group configuration mode. ● Enable inter-radio number balancing.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)#ap-group default AC(config-group)#inter-radio-balance num-balance enable
Verification	● Run the **show run** command and check the configurations.
AC	AC# show run | begin ap-group default ap-group default inter-radio-balance num-balance enable

Common Errors

- N/A

2.4.5 Configuring Association Control

Configuration Effect

- Secondary STAs must be associated with APs in the same group as the primary STA when being associated.

Notes

- When a package is deleted, all its related configurations are deleted as well. If some STAs in this package are currently associated, all these STAs will be disassociated.
- A package can only be configured with one primary STA. If the information about the primary STA in the package is configured for multiple times, the latest configuration prevails.
- When a primary STA is deleted from a package, the primary STA and all secondary STAs in this package may be disassociated.
- When a secondary STA is deleted from a package, this secondary STA may be disassociated.
- The association control zone name cannot be duplicated; otherwise, an error will be prompted. In addition, if an association control zone is deleted, all configurations related to this zone will be deleted. Consequently, STAs in the package associated with this control zone may be disassociated.
- When the AP information in an association control zone is deleted, STAs in the package associated with this AP be disassociated.

Configuration Steps

Configuring a Package

- (Mandatory) The configuration is performed on an AC or a fat AP.
- The primary and secondary STA information can be configured only after a package is configured.

Command	**package** *pkg-name*
Parameter Description	*pkg-name*: Indicates the name of a package. The package name is a string of 1 to 32 characters.
Defaults	No package is configured by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Primary and Secondary STAs in a Package

- (Mandatory) The configuration is performed on an AC or a fat AP.
- Run the **primary-sta** command to configure the primary STA. Only one primary STA can be configured. The secondary STAs will be associated with APs in the same group as the primary STA.
- Run the **secondary-sta** command to configure a secondary STA. After the secondary STA is configured, the secondary STA will be associated with an AP in the same group as the primary STA.

Command	**primary-sta** *mac-address*
Parameter Description	*mac-address*: Indicates the MAC address of the STA.
Defaults	No primary STA is configured by default.
Command Mode	Package configuration mode
Usage Guide	N/A

Command	**secondary-sta** *mac-address*
Parameter Description	*mac-address*: indicates the MAC address of the STA.
Defaults	No secondary STA is configured by default.
Command Mode	Package configuration mode
Usage Guide	-

Configuring an Association Control Zone

- (Mandatory) The configuration is performed on an AC or a fat AP.
- Configure an association control zone.
- APs can be added to an association control zone only after this association control zone is configured.

Command	**control-zone** *czone-name*
Parameter Description	*czone-name*: Indicates the name of an association control zone. The name is a string of 1 to 64 characters.
Defaults	No association control zone is configured by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Adding an AP to an Association Control Zone

- (Mandatory) The configuration is performed on an AC or a fat AP.
- Add an AP to an association control zone.
- Association control can be performed on only APs that are added to the association control zone.

Command	**ap** *WORD*
Parameter Description	*WORD*: Indicates the name of an AP. The name is a string of 1 to 64 characters.
Defaults	No AP is added to an association control zone by default.
Command Mode	Association control zone configuration mode
Usage Guide	N/A

Enabling the Association Control Function

- (Mandatory) The configuration is performed on an AC or a fat AP.The **assoc-control** command must be used to enable the association control function.
- Enable the association control function.

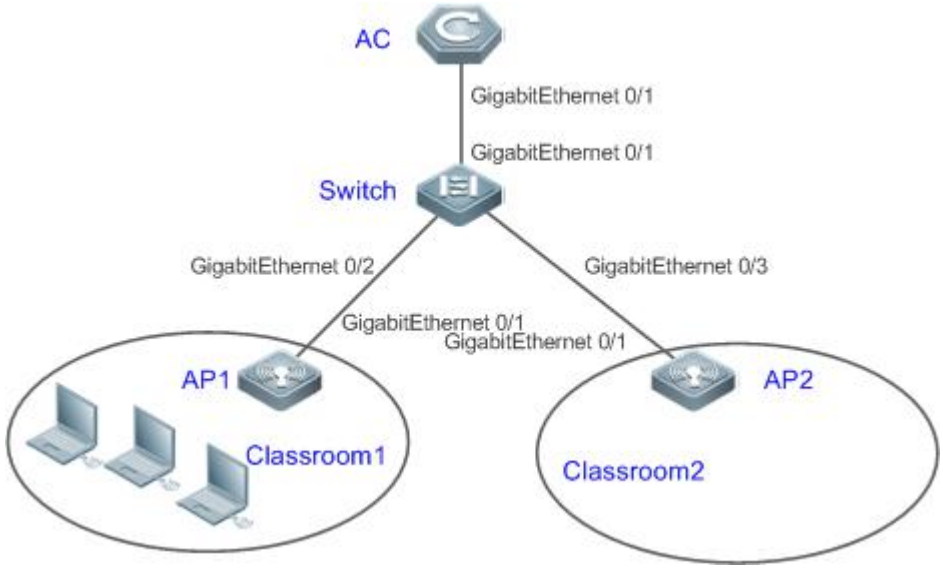
Command	**assoc-control**
Parameter Description	N/A
Defaults	The association control function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Verify that secondary STAs can be associated with APs in the same group as the primary STA.

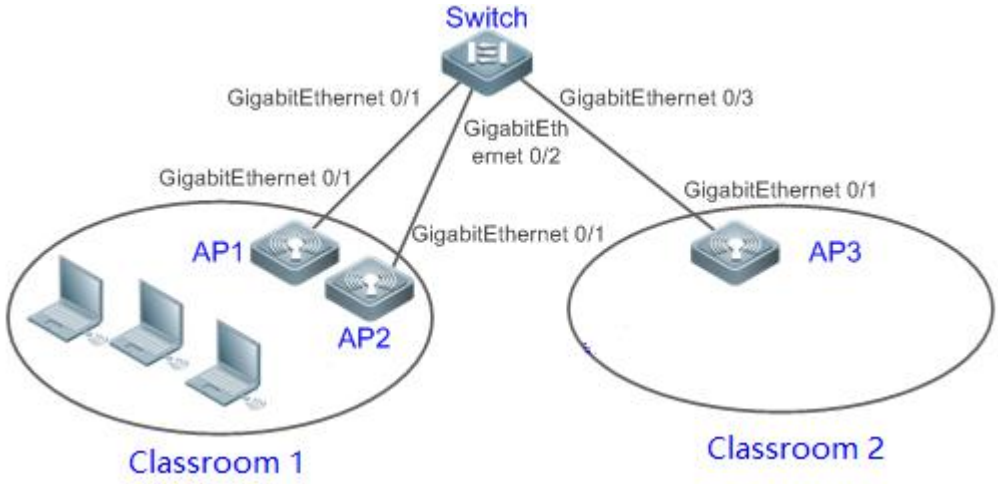
Configuration Example

Configuring the E-bag in Fit AP Structure.

Scenario **Figure 2-8**	
Configuration Steps	• Configure packages and related primary STAs and secondary STAs. • Configure association control zones and related APs. • Enable the association control function.
AC	AC#configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# package Cart 1 AC(config-package)#primary-sta 00d0.f800.0001 AC(config-package)#secondary-sta 00d0.f800.0002 AC(config-package)#secondary-sta 00d0.f800.0003 AC(config-package)#exit AC(config)# control-zone Classroom 1 AC(config-czone)#apAP1 AC(config-czone)#exit AC(config)# control-zone Classroom 2 AC(config-czone)# apAP2 AC(config-czone)#exit AC(config)#assoc-control

Verification	● Display the association control running state. ● Display the package configuration. ● Display the association control zone configurations.
AC	AC#show assoc-control Association control is enabled. AC# show package total package num : 1 ========= Cart 1 ========= primary STA : 00d0.f800.0001 secondary STA num : 2 00d0.f800.0002 00d0.f800.0003 AC# show control-zone control zone num : 2 control-zoneAP ---------- ---------- Classroom 1 AP1 00d0.f800.889e Classroom 2 AP2 00d0.f800.889f

Configuring the E-bag in Fat AP Structure.

Scenario **Figure 2-9**	
Configuration Steps	● Configure packages and related primary STAs and secondary STAs. ● Configure association control zones and related APs. ● Enable the association control function.
AP1	AP1# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AP1(config)# package Cart 1

	AP1(config-package)# primary-sta 00d0.f800.0001 AP1(config-package)# secondary-sta 00d0.f800.0002 AP1(config-package)# secondary-sta 00d0.f800.0003 AP1(config-package)# exit AP1(config)# control-zone Classroom 1 AP1(config-czone)# ap AP1 AP1(config-czone)# exit AP1(config)# assoc-control
AP3	AP3# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AP3(config)# package Cart 1 AP3(config-package)# primary-sta 00d0.f800.0001 AP3(config-package)# secondary-sta 00d0.f800.0002 AP3(config-package)# secondary-sta 00d0.f800.0003 AP3(config-package)# exit AP3(config)# control-zone Classroom 2 AP3(config-czone)# ap AP3 AP3(config-czone)# exit AP3(config)# assoc-control
Verification	● Display the association control running state. ● Display the package configuration. ● Display the association control zone configurations.
AP1	AP1# show assoc-control Association control is enabled. AP1# show package total package num : 1 ========= Cart 1 ========= primary STA : 00d0.f800.0001 secondary STA num : 2 00d0.f800.0002 00d0.f800.0003 AP1# show control-zone control zone num : 1 control-zone AP

	---------- ---------- Classroom 1 AP1 00d0.f800.889e
AP3	AP3# show assoc-control Association control is enabled. AP3# show package ========= Cart 1 ========= primary STA : 00d0.f800.0001 secondary STA num : 2 00d0.f800.0002 00d0.f800.0003 AP3# show assoc-control control zone num : 1 control-zone AP ---------- ---------- Classroom 1 AP3 00d0.f800.889f

Common Errors

- N/A

2.4.6 Configuring STA Management

Configuration Effect

- STAs are disassociated if no traffic is detected on the STAs within the specified time.

Notes

- N/A

Configuration Steps

Configuring the STA Aging Time

- (Optional) The configuration is performed on an AC or a fat AP.
- A shorter time configured indicates that an STA without traffic can be detected and disassociated in a faster manner.

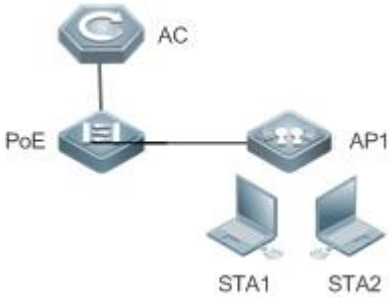
Command	**sta-idle-timeout** *value*
Parameter Description	*value*: Indicates the aging time in second. The value ranges from 60 to 86400.
Defaults	300s
Command Mode	AP configuration mode
Usage Guide	N/A

Verification

- Check whether the STA aging time is successfully configured.

Configuration Example

Configuring the STA Aging Time

Scenario Figure 2-10	
Configuration Steps	● Configure the STA aging time.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# ap-config ap1 AC(config-ap)# sta-idle-timeout 15
Verification	● After the CAPWAP tunnel is established between an AP and an AC, check the configuration information.
AC	AC# show ap-config running ap-config ap1 sta-idle-timeout 15 !

Common Errors

- N/A

2.4.7 Configuring STA Informational Syslog Suppression

Configuration Effect

- Even STAs are frequently associated or disassociated, the number of informational syslogs output per second does not exceed the limit.

Notes

- N/A

Configuration Steps

Configuring the Syslog Suppression Rate

- (Optional) The configuration is performed on the AC.
- Configure the syslog suppression rate. A larger rate configured indicates that more syslogs can be output per second.

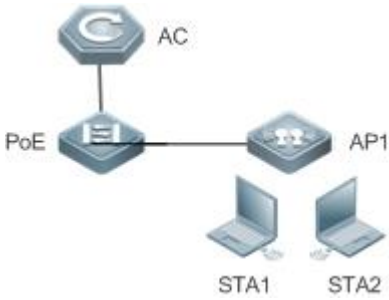
Command	**sta-logging rate-limit** *limit-num*
Parameter Description	*limit-num*: Indicates the rate, which is expressed in records per seconds. The value ranges from 0 to 10000.
Defaults	By default, less than five syslog records are output per second, that is, the maximum syslog output rate is 5 records per second.
Command Mode	AC configuration mode
Usage Guide	N/A

Verification

- Run the **show running** command to check whether the syslog suppression rate is successfully configured.

Configuration Example

Configuring the STA Informational Syslog Suppression Function

Scenario **Figure 2-11**	
Configuration Steps	● Configure the STA informational syslog suppression function.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# ac-controller AC(config-ac)# sta-logging rate-limit 50
Verification	● After the CAPWAP tunnel is established between an AP and an AC, check the configuration information.

AC	AC# show running ac-controller sta-logging rate-limit 50 !

Common Errors

- N/A

2.5 Monitoring

Displaying

Description	Command
Displays the detailed information about a specified STA.	**show ac-config client detail** *mac-address*
Displays the statistics of all STAs.	**show ac-config client statistic**
Displays the detailed configuration of the traffic-based balancing group.	**show ac-config flow-balance summary**
Displays the detailed configuration of the number-based balancing group.	**show ac-config num-balance summary**
Displays the status of the association control function.	**show assoc-control**
Displays the association control zone configuration.	**show control-zone** [**summary** | *czone-name*]
Displays the package configuration.	**show package** [*pkt-name*]
Displays the STAs in the blacklist.	**show sta-blacklist**

3 Configuring CAPWAP

3.1 Overview

Control And Provisioning of Wireless Access Points (CAPWAP) is a protocol proposed to address the issue of large-scale access point (AP) deployment on the wireless local area network (WLAN).

On a fit AP network, the access controller (AC) manages all APs in a unified manner through CAPWAP. The AC pushes control polices to specified APs, instead of configuring APs one by one. CAPWAP is used to set up the control channel and the data channel between an AP and an AC. The control channel is used by ACs to configure APs, or by APs to send event notifications to ACs. The data channel is used to exchange data packets between APs and ACs.

Protocols and Standards

- RFC5415: Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification
- RFC5416: Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11
- RFC5417: Control And Provisioning of Wireless Access Points (CAPWAP) Access Controller DHCP Option

3.2 Applications

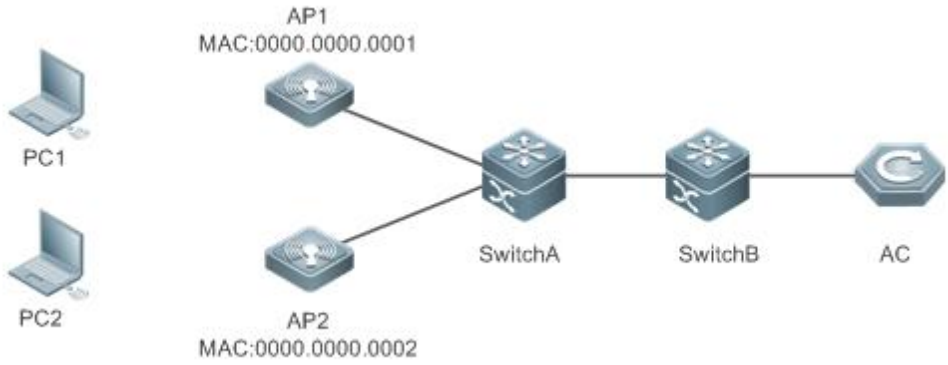
Application	Description
Dynamically Setting up a CAPWAP Tunnel	An AP accesses an AC through switches. The DCHP server is deployed on the switch connected to APs. The AP obtains the AC address dynamically through DHCP to set up a CAPWAP tunnel with the AC.
Statically Setting up a CAPWAP Tunnel	An AP accesses an AC through switches. The static IP address of the AC is configured on the AP. The AP sets up a CAPWAP tunnel with the AC based on the configured static IP address of the AC.
Upgrading APs	After a CAPWAP tunnel is set up between an AC and each AP, the AC upgrades APs in a large scale through CAPWAP.

3.2.1 Dynamically Setting up a CAPWAP Tunnel

Scenario

APs access the AC through switches. The DCHP server is deployed on the switch connected to APs. On the DHCP server, the DHCP address pool is configured and Option138 is pushed, where Option138 is the IP address of the AC. The AP obtains the AC address and sets up a CAPWAP tunnel with the AC. As shown in Figure 3-1, the AC, switches (SwitchA and SwitchB), and APs (AP1 and AP2) are connected with each other through the trunk ports. PC1 is connected to AP1, and PC2 is connected to AP2.

Figure 3-1



Deployment

- APs do not need to be configured one by one on a fit AP network. When an AP is powered on, the IP address must be obtained first. Therefore, a DHCP server must be deployed on the network. If the DHCP server is not deployed, the DHCP function of the AC is used to implement functions of the DHCP server.
- The AC communicates with the AP through the Layer3 (L3) switch, and the DHCP server must send Option138, which contains the IP address of the AC. After obtaining the IP address of the AC, the AP sets up a CAPWAP communication tunnel with the AC.
- On the AC, configure a loopback interface address, or run the **capwap ctrl-ip** *ip-address* command to configure the source address for setting up a CAPWAP tunnel.
- Configure a route to implement interworking between the AC and the IP address obtained by the AP.

3.2.2 Statically Setting up a CAPWAP Tunnel

Scenario

The AP sets up a CAPWAP tunnels with the AC based on the configured static IP address of the AC. An AP accesses an AC through switches. The topology is the same as that shown in Figure 3-1.

Deployment

- Configure the static IP addresses of ACs. The AP will send the Discover Request messages to these static IP addresses to check the effectiveness of ACs, and then select and join an AC.
- On the AC, configure a loopback interface address as the source address for setting up a CAPWAP tunnel.
- Configure a route to implement interworking between the AC and the IP address obtained by the AP.

3.2.3 Upgrading APs

Scenario

The AP obtains the AC address based on the configured static IP address of the AC or from the DHCP server, and sets up a CAPWAP tunnel with the AC. The AP accesses the AC through switches. The topology is the same as that shown in Figure 3-1.

Deployment

- On the AC, configure an IP interface address as the source address for setting up a CAPWAP tunnel.
- Configure a route to implement interworking between the AC and the IP address obtained by the AP.
- On the AC, activate the AP software that is stored locally.

3.3 Features

Basic Concepts

↘ STA, AP, and AC

STA: It is a wireless workstation that is equipped with the wireless network interface card (NIC), such as a laptop computer or a mobile phone.

AP: It is a wireless access point that provides radio signals so that the STA can access the wireless network.

AC: It is a wireless access controller that provides wireless connection and related service functions.

↘ Control Channel and Data Channel

Control channel: It is used by ACs to configure APs, or by APs to send event notifications to ACs.

Data channel: It is used to exchange data packets between APs and ACs.

AC Discovery

AC discovery phase: An AP can send a discover request message by means of broadcast, multicast, DHCP, DNS, or static configuration to detect ACs, select an optimum AC from one or more ACs, join the AC, and set up a CAPWAP session with the AC.

Datagram Transport Layer Security (DTLS)

The CAPWAP control channel uses the DTLS protocol for key negotiation and encryption.

Option

The Option information sent by the DHCP server can carry the IPv4 address of an AC. The AP obtains the AC address from the Option information sent by the DHCP server.

The AP can obtain the IP address of an AC using Option 138 or Option 43. When configuring the DHCP server of the AP, you must configure the related options to set the IP address of the AC; otherwise, the AP cannot discover the AC through DHCP discovery.

Option 138 and Option 52 are standard formats defined in RFC5417, and Option 43 is defined by vendors. Currently, Option 43 in the following formats can be analyzed:

Format 1: Assume that the IP address of a specified AC is 1.1.1.1. The corresponding configuration is Option 43 hex f10401010101.

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   option-code   | option-length | Sub-opt Type   |   Sub-opt Len   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Server   Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

option-code: indicates the option code. In this example, the option code is 43 in decimal format.

option-length: indicates the length of the option data, which excludes option-code and option-length.

Sub-opt Type: indicates the sub-option type. In this example, the sub-option type is 0xF1, that is, 241 in decimal format.

Sub-opt Len: indicates the length of the sub-option, which is equal to (Number of addresses x 4).

Server Address: indicates the server address.

Format 2: Assume that the IP address of a specified AC is 1.1.1.1. The corresponding configuration is option 43 hex 800700000101010101.

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   option-code   | option-length | Sub-opt Type   |   Sub-opt Len   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            PXE Server Type            | PXE Server Num|                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
          PXE Server   Address                          |        …            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

option-code: indicates the option code. In this example, the option code is 43 in decimal format.

option-length: indicates the length of the option data, which excludes option-code and option-length.

Sub-opt Type: indicates the sub-option type. In this example, the sub-option type is 0x80, that is, 128 in decimal format.

Sub-opt Len: indicates the length of the sub-option, which is equal to (Number of addresses x 4 +3).

Server Type: indicates the server type. The value is 0x0000.

Server Num: indicates the number of server addresses.

Server Address: indicates the server address.

Format 3: Assume that the IP address of a specified AC is 1.1.1.1. The corresponding configuration is option 43 hex 01010101.

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   option-code   |option-length|Server   Address            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Server   Address            |                 …   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

option-code: indicates the option code. In this example, the option code is 43 in decimal format.

option-length: indicates the length of the option data, which excludes option-code and option-length.

Server Address: indicates the server address.

Overview

Feature	Description
Discovering an AC by an AP	The AP discovers potential ACs.
Joining an AC by an AP	The AP selects an optimum AC from one or more ACs, joins the AC, and sets up a CAPWAP tunnel with the AC.
Upgrading APs	After a CAPWAP tunnel is set up between an AC and each AP, the AC upgrades APs in a large scale.
Forwarding Data on the Tunnel	After a CAPWAP tunnel is set up between an AC and each AP, data packets can be exchanged through the data channel.

3.3.1 Discovering an AC by an AP

An AP discovers potential ACs by sending a Discovery Request message.

Working Principle

As soon as an AP is connected to the network, the AP enters the process of discovering ACs. The AP sends a Discovery Request message by means of broadcast, multicast, or unicast If unicast is used, the AP obtains the AC IP address list through the DHCP server, DNS, or configuration of the static AC IP addresses.

3.3.2 Joining an AC by an AP

The AP selects an optimum AC from one or more ACs, joins the AC, and sets up a CAPWAP tunnel with the AC.

Working Principle

The AP sends a Discovery Request message to ACs. ACs that receive the Discovery Request message return a Discovery Response message to the AP. Among the ACs that send the response message, the AP selects an optimum AC, and sets up a DTLS connection with

this AC. After the DTLS connection is successfully set up, the AP sends a Join Request message. The AC returns a Join Response message to confirm that the AP is added to the management scope of the AC, and starts to provide services for this AP.

3.3.3 Upgrading APs

After a CAPWAP tunnel is set up between an AC and each AP, the AC upgrades APs in a large scale.

Working Principle

After an AP joins an AC, if the AP firmware version expires, the AP enters the firmware upgrade process. The AP downloads the latest firmware version from the AC, restarts after the successful upgrade, and reinitiates an AC discovery process. If the AP firmware is of the latest version, the AP downloads configuration parameters from the AC and starts running. Figure 3-2 shows the working principle.

Figure 3-2

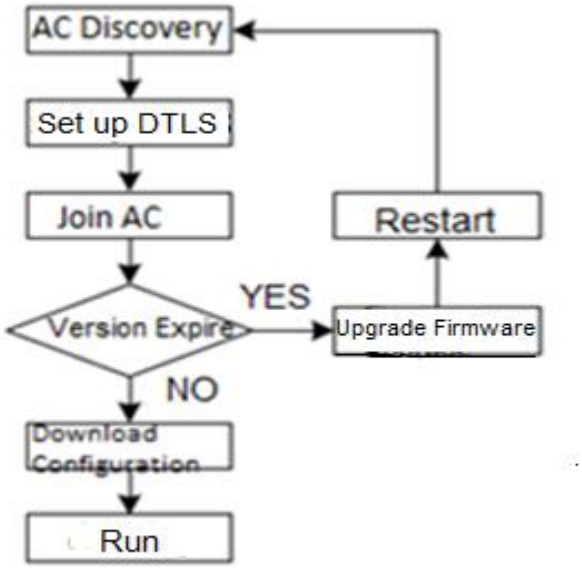
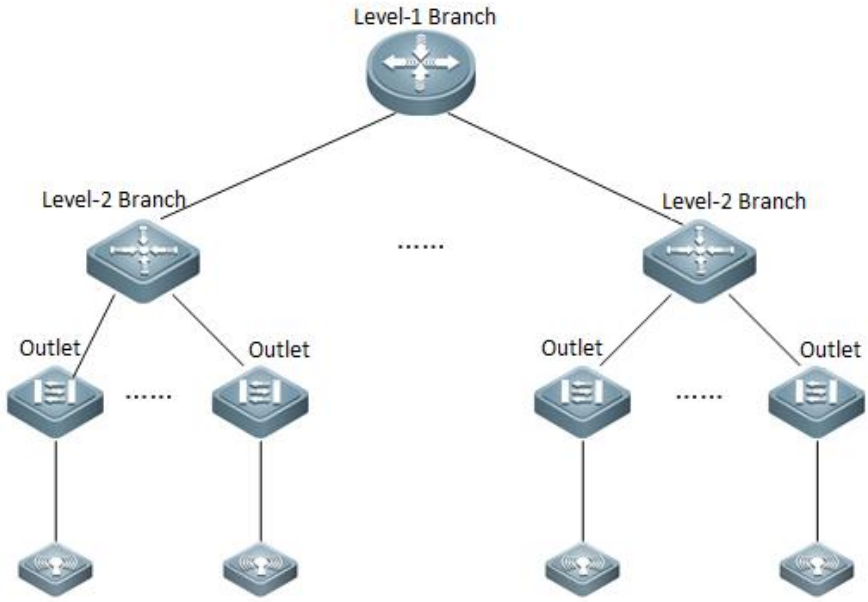


Figure 3-3 shows the typical upgrade scenario where the bandwidth is limited.

Figure 3-3



The following explains the configuration method for upgrading APs in a bank. Assume that the bank consists of one level-1 branch and multiple level-2 branches, and each branch has hundreds of outlets. One AP is deployed in one outlet, and the AC is deployed in the level-1 branch. The bandwidth between the level-1 bank and the level-2 bank is 20 Mbps, and the bandwidth between the level-2 bank and the outlet is 2 Mbps. To prevent affecting normal service provisioning of the bank, the bandwidth occupied by the AP upgrade process cannot exceed 50% of the total available bandwidth. Assume that there are eight level-2 branches, eight upgrade groups are configured on the AC, and APs of outlets under each level-2 branches are added to the corresponding upgrade group. For each AP, the maximum available bandwidth is 1 Mbps. Therefore, a bandwidth of 128 Kbps (1MByte = 128KByte) should be configured for each AP. Under each level-2 branch, the number of APs that can be upgraded concurrently is 10 (10 Mbps/1 Mbps). In addition, it is recommended that the maximum number of APs that can be concurrently upgraded by an AC be set to the number of upgrade groups multiplied by the number of APs that can be upgraded concurrently in a upgrade group, that is, 80.

3.3.4 Forwarding Data on the Tunnel

After a CAPWAP tunnel is set up between an AC and each AP, data packets can be exchanged over the data channel.

Working Principle

The CAPWAP sets up a control channel and a data channel between APs and ACs. The control channel is used by ACs to configure APs, or by APs to send event notifications to ACs, and must be encrypted. The data channel is used to exchange the 802.11 or 802.3 frames between APs and ACs. When running on the IPv4 protocol stack, the CAPWAP uses the UDP for data transmission.

3.4 Configuration

Configuration	Description and Command	
Configuring the AC Location	(Optional) It is used to configure the location information of an AC.	
	location	Configures the location information of an AC so that the physical location of the AC can be viewed.
Configuring the version number	(Optional) It is used to configure the version number.	
	set-version	Configures the version number,

Configuring the AP Location	(Optional) It is used to configure the location information of an AP.	
	location	Configures the location information of an AP so that the physical location of the AP can be viewed.
Configuring AP Time Synchronization	(Optional) It is used to enable the AP to synchronize the time with the AC.	
	timestamp	Enables the AP to synchronize the time with the AC.
Configuring the Default VLAN of an AP	(Optional) It is used to configure the native VLAN of an AP.	
	ap-vlan	Configures the default VLAN of an AP.
Configuring the VLAN of AP Wired Users	(Optional) It is used to configure the VLAN of wired users when the AP provides an Ethernet interface for access of wired users.	
	wired-vlan	Configures the VLAN used by the wired network port.
Configuring the Wired Network Port Status of an AP	(Optional) It is used to disable wired network ports when the AP provides Ethernet ports for access of wired users.	
	wired-interface	Disables wired network ports of an AP.
Configuring the Sub-Interface of the WAN Interface on the AP	(Optional) It is used to configure the sub-interface of the WAN interface on the AP.	
	ap-subif	Configures the sub-interface of the WAN interface on the AP.
Configuring Data to Allow an AP to Join an AC	(Optional) It is used to configure an AP on the AC to set up a CAPWAP tunnel.	
	ac-domain-name	Configures the DNS domain name of the AP, which is used to obtain the AC address.
	acip ipv4	Configures the static IP address of the AC accessed by the AP.
	ip address	Configures the static IP address, subnet mask, and gateway.
Configuring an AP via an AC	(Optional) It is used to configure an AP via an AC.	
	exec-cmd	Executes ap-config commands on an AP/AP group via an AC.
Configuring a Fit AP	(Optional) It is used to perform pre-configuration on an AP to set up a CAPWAP tunnel.	
	acip ipv4	Configures the static IP address of the AC accessed by the AP.
	apip	Configures the static IP address, subnet mask, and gateway.
	apip pppoe	Enables the AP to use the PPPoE dial-up mode to obtain the address.
Configuring AP Upgrade	(Optional) It is used to configure the AP upgrade data.	
	ap-serial	Creates the name of an AP product series, and specifies the AP product models that belong to this series.

	ap-image	In AP configuration mode, configures the specified AP upgrade version. In AC configuration mode, configures the specified AP software version that should be used by a specified AP product series for the upgrade, or sets the adaptive upgrade mode.
	active-bin-file	Activates the AP software version file.
	capwap upgrade max-concurrent	Configures the maximum number of APs that can be concurrently upgraded by the AC.
	capwap upgrade group	In AC configuration mode, creates a bandwidth control upgrade group.
	ap-upgrade band-width	In AC configuration mode, configures the bandwidth for centralized AP upgrade.
	ap-upgrade group	In AC configuration mode, adds APs to the bandwidth control upgrade group.
Configuring the CAPWAP Control Address	(Optional) It is used to configure the control IP address of the CAPWAP tunnel. When this address is not configured, the address of the loopback interface is used as the control IP address by default.	
	capwap ctrl-ip	Configures the control IP address of the CAPWAP tunnel.
Configuring CAPWAP Fragmentation	(Optional) It is used to configure CAPWAP fragmentation.	
	capwap mtu	Configures the maximum transmission unit (MTU) on the tunnel of a specified AP.
	capwap fragment enable	Enables CAPWAP fragmentation for a specified AP.
Configuring CAPWAP Encryption	(Optional) It is used to configure CAPWAP encryption.	
	capwap dtls enable	Enables encryption on the CAPWAP control channel.
Configuring CAPWAP Access Control	(Optional) It is used to control the maximum number of APs that can concurrently go online.	
	capwap max-concurrent	Configures the maximum number of APs that can concurrently go online.
Configuring the Echo Interval of the CAPWAP Tunnel	(Optional) It is used to configure the echo interval of the CAPWAP tunnel.	
	echo-interval	Configures the echo interval of the CAPWAP tunnel.
Configuring the Maximum Retransmission Times of a CAPWAP Packet	(Optional) It is used to configure the maximum transmission times of a CAPWAP packet.	
	capwap max-retransmit	Configures the maximum transmission times of a CAPWAP packet.

3.4.1 Configuring the AC Location

Configuration Effect

- Configure the location information of an AC so that users can conveniently check the locations of ACs on the WLAN.

Notes

- The location information is a string of 1 to 255 characters, and cannot contain any space.

Configuration Steps

- (Optional) Configure the AC location so that users can conveniently check the locations of ACs when a large number of ACs exist on the network.
- Enter the AC configuration mode, and run the **location** command to configure the AC location on the AC.
- Use the **no** form of this command to restore the default setting.

Command	**location** *location-string*
Parameter Description	*location-string*: indicates the location of an AC. The location is a string of 1 to 255 characters, and cannot contain any space.
Defaults	FS_COM
Command Mode	AC configuration mode
Usage Guide	The AC location information is FS_COM by default. You can configure the location information for each AC according to actual requirements so that you can conveniently check the AC location on the WLAN.

Verification

- Run the **show ac-config** command to display the AC location information and accordingly determine whether the configuration is successful.

Configuration Example

Configuring the AC Location Information as "computer-layer2"

Configuration Steps	• Enter the AC configuration mode. • Configure the AC location information.
AC	FS(config)#ac-controller FS(config-ac)# locationcomputer-layer2
	• Use the **no** form of this command to restore the default AC location information.
AC	FS(config)#ac-controller FS(config-ac)#no location
Verification	Run the **show ac-config** command to display the current location of the AC.
AC	FS#show ac-config ac location :Ac_COM

Common Errors

- N/A

3.4.2 Configuring the Version Number

Configuration Effect

- Customize the firmware version.

Notes

- The customized version number contains a maximum of 63 characters.

Configuration Steps

- Optional.
- Run this command to configure the customized firmware version number.
- Use the **no** form of this command to restore the default settings.

Command	**set-version** *string*
Parameter Description	*string*: indicates the customized version number.
Defaults	N/A
Command Mode	AC configuration mode
Usage Guide	This command is used to configure the firmware version number of the AC and push the firmware version number to APs.

Verification

- Run the **show version** command to display the version number.

Configuration Example

Configuring the Customized Firmware Version Number to FSOS 10.4(2B17)-SP2

Configuration Steps	Enter the AC configuration mode. Configure the customized version number.
AC	FS(config)#ac-controller FS(config-ac)# set-version FSOS 10.4(2B17)-SP2
Verification	Run the **show version** command to display the version number.
AC	FS#show version System software version : FSOS 10.4(2B17)-SP2

Common Errors

N/A

3.4.3 Configuring the AP Location

Configuration Effect

- Configure the location information of an AP.

Notes

- The AP location information is a string of 1 to 255 characters, and cannot contain any space.

Configuration Steps

Configuring the AP Location Information

- Optional.
- Run the **location** command to configure the AP location information.
- You can enter the AP configuration mode and configure the AP location information on the AC so that you can conveniently learn the physical location of the AP.

Command	**location***location-string*
Parameter Description	*location-string*: indicates the location of an AP. The location is a string of 1 to 255 characters, and cannot contain any space
Defaults	Null
Command Mode	AP configuration mode
Usage Guide	N/A

Verification

- Run the **show ap-config running** command to display the AP location information.

Configuration Example

Configuring the Location Information of AP0001 as "AP-company"

Configuration Steps	• Enter the AP configuration mode on the AC. • Configure the location information of AP0001 as "AP-company".
AC	FS(config)# ap-config AP0001 FS(config-ap)# location AP-company
Verification	• Run the **show ap-config running** command to display the location information of AP0001.
AC	FS#show ap-config running ! ap-config AP0001 location AP-company !

Common Errors

- N/A

3.4.4 Configuring AP Time Synchronization

Configuration Effect

- Enable a specified AP or all APs in an AP group to synchronize the time with the AC.

Notes

- N/A

Configuration Steps

Enabling a Specified AP or All APs in an AP Group to Synchronize the Time with the AC

- Optional.
- To synchronize the time on the AP with that on AC, enter the AP or AP group configuration mode on the AC and run the **timestamp** command.

Command	**timestamp**
Parameter Description	N/A
Defaults	N/A
Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	N/A

Verification

- Check whether the time on the AC is the same as that on the AP.

Configuration Example

Enabling AP0001 to Synchronize the Time with the AC

Configuration Steps	• Enter the AP configuration mode on the AC. • Enable AP0001 to synchronize the time with the AC.
AC	FS(config)# ap-config AP0001 FS(config-ap)# timestamp
Verification	• Run the **show clock** command to display the time on the AP0001 and the AC.
AC	FS#showclock 16:41:05 UTC Thu, Oct 17, 2013

Common Errors

- N/A

3.4.5 Configuring the Default VLAN of an AP

Configuration Effect

- The AP automatically removes the TAG from a frame that contains the native VLAN before forwarding the frame. That is, in local forwarding mode, when the VLAN of the user is the same as the native VLAN, the frame of the user does not contain the TAG when forwarded, and the access switch determines the VLAN to which the user belongs.

Notes

- After this command is executed, an online AP will go offline and then the connection will be set up again.
- When a wireless distribution system (WDS) is deployed, the same AP-VLAN must be planned for the ROOT-BRIDGE and NONROOT-BRIDGE devices; otherwise, the NONROOT-BRIDGE devices cannot share the same address pool with the ROOT-BRIDGE devices or the NONROOT-BRIDGE devices cannot even forward packets properly.
- This command is configured only in local forwarding mode when both the VLANs of STAs on a WLAN and APs must be determined by the access switch, whereas STAs on another WLAN must belong to VLAN 1 but the native VLAN of the access switch is not VLAN 1. Generally, this configuration is not required.
- If the static DHCP address pool is configured, and the client ID is specified to use Bridge-Group Virtual Interface (BVI) 1, configuration of this command will change the BVI interface of the AP. In this case, the DHCP server configuration must be modified; otherwise, the address cannot be obtained.
- If the AP uses the PPPoE dial-up mode to obtain the address, the CAPWAP module on the AP will select dialer 1 as the source interface, and the STA traffic will be forwarded without containing the TAG. Therefore, this command is meaningless.

Configuration Steps

Configuring the Default VLAN of an AP

- Optional.
- When planning of the users' native VLANs is required, you can configure the same VLAN as the default VLAN of an AP and the VLAN of the user. In this way, both the VLAN of the user and the VLAN of the AP are determined by the access switch.

Command	**ap-vlan** *vlan-id*
Parameter Description	*vlan-id*: indicates the ID of the specified VLAN. The VLAN ID ranges from 1 to 4094. The default value is 1.
Defaults	1
Command Mode	AP configuration mode or all AP (ap-config all) configuration mode
Usage Guide	The AP automatically removes the TAG from a frame that contains the native VLAN before forwarding the frame. That is, in local forwarding mode, when the VLAN of the user is the same as the native VLAN, the frame of the user does not contain the TAG when forwarded, and the access switch determines the VLAN to which the user belongs.

Verification

- Run the **show running** command to display the configurations of all APs, or the **show ap-config running** command to display the configurations of a specified AP.

Configuration Example

Setting the VLAN ID of the Native VLAN of AP1 to 20

Configuration Steps	● Enter the AP configuration mode on the AC. ● Set the VLAN ID of the native VLAN of AP1 to 20.
AC	FS(config)# ap-config AP1 FS(config-ap)# ap-vlan20
Verification	● Run the **show ap-config running** command to display the location information of AP1.
AC	FS#show ap-config running ! ap-config AP1 ap-vlan 20 !

Common Errors

According to the planning, the native VLAN of the switch is VLAN 20, and all wireless/wired users and APs belong to VLAN 20. The following configurations are incorrect:

On the AC:

```
FS(config)# ap-configAP120
FS(config-ap)# wired-vlan20
FS(config-ap)# exit
FS(config)#wlan-config 1 ssid
FS(config-wlan)#tunnel local
FS(config-wlan)#exit
FS(config)#ap-group default
FS(config-ap-group)#interface-mapping 1 20 radio 1
```

On the switch:

```
FS(config)#interface GigabitEthernet 0/1
FS(config-if-GigabitEthernet 0/1)# switchport mode trunk
FS(config-if-GigabitEthernet 0/1)#switchport trunk native vlan 20
```

The configurations here are incorrect because the VLAN of users is different from the native VLAN of APs. Therefore, the uplink packets of APs contain TAG 20 when forwarded, and the access switch transparently forwards VLAN 20 and assigns addresses to users. As the native VLAN of the switch is VLAN 20, the downlink packets do not contain the TAG when forwarded. The Native VLAN of APs is 1 by default. Therefore, the packets cannot be forwarded to users, and the wireless and wired users cannot obtain their addresses.

Either of the following methods can be used to modify the configurations:

Method 1: Change **wired-vlan 20** to **wired-vlan 1** and **interface-mapping 1 20 radio 1** to **interface-mapping 1 1 radio 1**, and the native VLAN of the switch remains unchanged.

Method 2: Add the native VLAN configurations for APs, and other configurations remain unchanged.

On the AC:

```
FS(config)# ap-configAP120
FS(config-ap)# ap-vlan 20
```

3.4.6 Configuring the VLAN of Wired Users

Configuration Effect

- Specify the VLAN of wired users when the AP provides an Ethernet interface for access of wired users.

Notes

- This command can be configured on all APs, but the configurations take effect only on APs that are equipped with the wired network ports.
- In wireless AP mode, the AP implements only the wireless access function, but does not assign addresses to users. In this mode, if the VLAN used by the wired network port is configured the same as the VLAN of the AP, the VLAN of the packets sent over the wired network port will be determined by the access switch, instead of the VLAN specified in this command. If the packets sent over the wired network port must contain the TAG when forwarded, the native VLAN of the access switch cannot be the same as the VLAN of the wired network port; otherwise, the packets cannot be forwarded to the wired network port.
- In wireless routing mode, the AP can assign addresses to users. In this mode, wired users obtain IP addresses from the DHCP address pool, and the VLAN of the interface of the address pool must be the same as the VLAN specified in this command.
- When the configurations of the wired network port are automatically saved on the AP and the VLAN of the wired network port is different from the native VLAN of the AP, the AP cannot obtain the IP address of the LAN interface on the AP after the AP is restarted, and management cannot be implemented through the wired network port. In this case, the RESET key of the AP can be pressed and held to restore the factory settings.

Configuration Steps

Configuring the Access VLAN of the AP Wired Network Port

- Optional.
- To plan VLANs so that the VLAN of a wired user is different from the VLAN of the AP, run the **wired-vlan** command on the AC.

Command	**wired-vlan** *vlan-id* [**port***port-id*] **auto-save**
Parameter Description	*vlan-id*: indicates the ID of the specified VLAN. The VLAN ID ranges from 1 to 4094. By default, the VLAN used by the wired network port is the same as the VLAN of the AP. *port-id:* indicates the ID of the wired network port. The value ranges from 1 to 4. **auto-save**: indicates that configurations are automatically saved on the AP. After the AP is restarted, the configurations can be restored.
Defaults	By default, the VLAN used by the wired network port is not configured, indicating that this VLAN is the same as the VLAN of the AP.
Command Mode	AP configuration mode, all AP configuration mode, or AP group configuration mode

Usage Guide	The fit AP is started without being configured, and its configurations are sent from the AC. The **auto-save** parameter can be configured to enable automatic saving of the wired network port configurations on the AP. In this way, when the AP is disconnected from the AC, the wired network port configurations can be restored after the AP is restarted, and users can still access the network through the wired network port.

Verification

- Run the **show running** command to display the configurations of all APs, or the **show ap-config running** command to display the configurations of a specified AP.

Configuration Example

Configuring VLAN 20 for the Wired Network Port of AP1

Configuration Steps	• Enter the AP configuration mode on the AC. • Configure VLAN 20 for the wired network port of AP1.
AC	FS(config)# ap-config AP1 FS(config-ap)# wired-vlan20
Verification	• Run the **show ap-config running** command to display the configurations of AP1.
AC	FS#show ap-config running ! ap-config AP1 wired-vlan 20 !

Common Errors

N/A

3.4.7 Configuring the Wired Network Port Status of an AP

Configuration Effect

- Enable or disable the wired network port of an AP.

Notes

- This command can be configured on all APs, but the configurations take effect only on APs that are equipped with the wired network ports.
- After the AP wired network port is disabled and the AP is restarted, management cannot be implemented through the wired network port. In this case, you can press and hold the RESET key of the AP to restore factory settings.

Configuration Steps

Configuring the Wired Network Port Status of an AP

- Optional.

- To enable or disable wired network ports of an AP, run the **wired-interface** command on the AC.

Command	**wired-interface** [**port** *port-id*] **enable**
Parameter Description	*port-id:* indicates the ID of the wired network port. The value ranges from 1 to 4. **enable**: indicates that the specified wired port is enabled.
Defaults	All the wired network ports are enabled by default.
Command Mode	AP configuration mode, all AP configuration mode, or AP group configuration mode
Usage Guide	The wired network ports of APs can be disabled when APs provide the Ethernet ports for access of wired users, but the application scenario does not require access to the wired network or deployment of the wired network is not completed yet.

Verification

- Run the **show running** command to display the configurations of all APs, or the **show ap-config running** command to display the configurations of a specified AP.

Configuration Example

Disabling All Wired Network Ports of AP1

Configuration Steps	• Enter the AP configuration mode on the AC. • Disable all wired network ports of AP1.
AC	FS(config)# ap-config AP1 FS(config-ap)# no wired-interfaceenable
Verification	• Run the **show ap-config running** command to display the configurations of AP1.
AC	FS#show ap-config running ! ap-config AP1 no wired-interfaceenable !

Common Errors

N/A

3.4.8 Configuring the Sub-Interface of the WAN Interface on the AP

Configuration Effect

- A wireless AP creates a sub-interface of the WAN interface by default so that the STA data contains the TAG when forwarded. In wireless routing mode that AP can assign addresses to users, the users' gateway is located on the AP, and the related packets do not need to contain the TAG when forwarded. Therefore, the **ap-subif enable** command can be used to delete the sub-interface of the WAN interface on the AP to prevent an address conflict caused by the same gateway address of STAs.

Notes

- If the AP obtains the address in PPPoE dial-up mode, the sub-interface of the WAN interface on the AP will be automatically deleted. In dial-up mode, this command cannot be used to configure the sub-interface of the WAN interface on the AP.

Configuration Steps

Configuring the Sub-interface of the WAN Interface on the AP

- Optional.
- In wireless routing mode, delete the sub-interface of the WAN interface on the AP; otherwise, an address conflict occurs when a large number of packets are forwarded through the sub-interface because the gateway addresses of users are the same.

Command	**ap-subif enable**
Parameter Description	N/A
Defaults	A sub-interface of the WAN interface is created by default.
Command Mode	AP configuration mode or all AP configuration mode
Usage Guide	N/A

Verification

- Run the **show running** command to display the configurations of all APs, or the **show ap-config running** command to display the configurations of a specified AP.

Configuration Example

Deleting the Sub-interface of the WAN Interface from AP1

Configuration Steps	• Enter the AP configuration mode on the AC. • Delete the sub-interface of the WAN interface from AP1.
AC	FS(config)# ap-config AP1 FS(config-ap)# no ap-subif enable
Verification	• Run the **show ap-config running** command to display the configurations of AP1.
AC	FS#show ap-config running ! ap-config AP1 no ap-subif enable !

Common Errors

N/A

3.4.9 Configuring Data to Allow an AP to Join an AC

Configuration Effect

- Configure the static IP addresses of ACs. The AP will send the Discover Request messages to these static IP addresses to check the effectiveness of ACs, and then select and joint an AC to set up a CAPWAP tunnel.

Notes

- A fit AP is generally not configured. It can discover ACs by means of broadcast, unicast, DHCP, or DNS, or join ACs based on the statically configured AC addresses.
- If the AP address is configured as the static address, the DHCP function will be disabled. In this case, the AC address cannot be obtained from the DHCP option. Therefore, before this command is configured, you need to configure the address of the connected AC in AP configuration mode so that the AP can discover and join the AC when the AP and the AC are not in the same subnet.

If the current address of the AP is different from the address specified in the AC command, the AP static address will be updated and the CAPWAP tunnel will be re-established. Configuration Steps

Configuring the Static AC Address

- Optional.
- The AC address can be obtained through DHCP or DNS. Alternatively, the static AC address can be configured in AP configuration mode on the AC or configured on the AP.
- When the AC address is obtained in static mode, run the **acip ipv4** command to configure the static AC address.

Command	**acip ipv4** *ip-address* [*ip-address*. . .]
Parameter Description	*ip-address*: indicates the static IP address. At most six static addresses can be configured.
Defaults	No static AC IP address is configured by default.
Command Mode	Global configuration mode on the AP or AP configuration mode on the AC
Usage Guide	N/A

Configuring the Domain Name Used by the AP to Discover the AC

- (Optional) Run the **ac-domain-name** command to configure the DNS domain name on the AC so that the AP can discover the AC based on the DNS domain name.
- When the AC address is obtained in dynamic mode, configure the DNS domain name on the AC. The AC address can be obtained based on the DNS domain name.
- Generally, if the DNS domain name is not configured, the AP cannot obtain the IP address of the AC through the DNS.

Command	**ac-domain-name***ac-domain-name*
Parameter Description	*ac-domain-name*: indicates the AC domain name.
Defaults	ac.FS.com.cn

Command Mode	AP configuration mode or AP group configuration mode on the AC
Usage Guide	N/A

Configuring the Static IP Address of the AP

- Optional.
- On the AP, configure the static IPv4 address of the AP so that the AP can use the fixed IPv4 address to access the AC.

Command	**ip address** *ip-address network-mask gateway*
Parameter Description	*ip-address*: indicates the IP address of the AP. *network-mask*: indicates the subnet mask of the AP. *gateway*: indicates the gateway of the AP.
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	An AP can obtain its own IP address through the static configuration or DHCP. If the static IP address is not configured on the AP, the AP obtains the address through DHCP and joins the AC. In this case, you can run this command to configure the static IP address of the AP so that the address can remain unchanged after the AP is restarted.

Verification

- Run the **show ap-config running** command to check whether the configuration is successful.

Configuration Example

Enabling the AP to Obtain the IP Address of the AC Based on the Static IPv4 Address of the AP

Configuration Steps	• Enter the AP configuration mode on the AC. • Set the static IP address of the AC accessed by the AP to 192.168.1.1. • Set the static IP address of the AP to 1.1.1.1, subnet mask to 255.255.255.0, and gateway to 1.1.1.2.
AC	FS(config)# ap-config AP0001 FS(config-ap)# acip ipv4 192.168.1.1 FS(config-ap)# ip address 1.1.1.1 255.255.255.0 1.1.1.2
Verification	• Check the AP configurations.
AC	FS#show ap-config running ! ap-config AP0001 acip ipv4 192.168.1.1 ip address 1.1.1.1 255.255.255.0 1.1.1.2 !

Enabling the AP to Obtain the IP Address of the AC based on the DNS Domain Name

Configuration Steps	● Enter the AP configuration mode on the AC. ● Set the DNS domain name of the AC to FS-ac.
AC	FS(config)# ap-config AP0001 FS(config-ap)# ac-domain-name FS-ac
Verification	● Check the AP configurations.
AC	FS#show ap-config running ! ap-config AP0001 ac-domain-name FS.ac !

Common Errors

- N/A

3.4.10 Configuring an AP to Execute a Command

Configuration Effect

- (Optional) On the AC, configure an AP to execute a command.
- (Optional) On the AC, configure all APs in an AP group to execute a command.

Notes

- N/A

Configuration Steps

Configuring an AP to Execute a Command

- (Optional) Enter the AP configuration mode.
- On the AC, configure the AP to execute a command.

Command	**exec-cmd mode** *exec-mode* **cmd** *exec-cmd* **once**
Parameter Description	*exec-mode*: indicates the mode in which a command is executed on the AP. *exec-cmd*: indicates the command to be executed on the AP. once: indicate the command is executed only once and not saved.
Defaults	N/A
Command Mode	Single AP configuration mode/All APs configuration mode
Usage Guide	Some configuration commands are supported currently only by the AP and they are unavailable on the AC. To configure the commands for APs on the AC, run the **exec-cmd** command. To cancel or change the

	configuration of the **exec-cmd** command, run the **no exec-cmd** command to remove the configuration and then run the **exec-cmd** command to cancel or change the required configuration.

Verification

- Log in to the AP to check whether the configuration takes effect. On the AC, run the **show run** or **show ap-config run** command to check whether the configuration takes effect.

Configuring APs in an AP Group to Execute a Command

- (Optional) Enter the AP group configuration mode.
- Configure all APs in an AP group to execute a command.

Command	**exec-cmd** *exec-cmd*
Parameter Description	*exec-cmd*: indicates the command to be executed on all APs in an AP group.
Defaults	N/A
Command Mode	AP group configuration mode.
Usage Guide	Some configuration commands are available only in AP configuration mode and they are unavailable in AP group configuration mode. To configure such a command for all APs in an AP group, run the **exec-cmd** command in the AP group. Note that the configuration is not saved in AP group configuration mode, that is, the command is executed only once on all APs in the current AP group. If the configuration already exists in AP configuration mode, the original configuration will be overridden when the command is executed in AP group configuration mode.

Verification

- Run the **show ap-config run** command to check whether the configuration of the APs in an AP group takes effect.

Configuration Example

Disabling the Eweb Function for an AP on the AC and Configuring Bluetooth iBeacon for all APs in an AP Group

Configuration Steps	• On the AC, disable the Eweb function for APs. • On the AC, enable the Eweb function for APs. • Enable Bluetooth iBeacon for all APs in an AP group. • Disable the Eweb function for all APs in the AP group.

AC	FS(config)#ap-config AP1 FS(config-ap)# exec-cmd mode configure cmd "no enable service web-server all" FS(config-ap)# no exec-cmd mode configure cmd "no enable service web-server all" FS(config-ap)# exec-cmd mode configure cmd "enable service web-server all" FS(config)#ap-group default FS(config-group)#exec-cmd ibeacon uuid ffffffffffffffffffffffffffffffff major ffff minor ffff FS(config-group)#exec-cmd exec-cmd mode configure cmd "no enable service web-server all"
Verification	● On the AC, check whether the configuration takes effect.
AC	FS#show ap-config running ap-config AP1 exec-cmd mode configure cmd "no enable service web-server all" ibeacon uuid ffffffffffffffffffffffffffffffff major ffff minor ffff

Common Errors

The **exec-cmd** command needs to be changed, but the **no exec-cmd** command is not executed to delete original configuration, or the **exec-cmd** command is not re-executed to cancel the configuration.

3.4.11 Configuring a Fit AP

Configuration Effect

- Configure the static IP address, subnet mask, next hop, and AC address on a fit AP so that the AP can use the static address to communicate with the AC.

Notes

- If the AP address is configured as the static address, the DHCP function will be disabled. In this case, the AC address cannot be obtained from the DHCP option. Therefore, you need to configure the address of the connected AC on the fit AP so that the AP can discover and join the AC when the AP and the AC are not in the same subnet.
- The fit AP configuration commands have the same functions as some AP configuration commands used on the AC. When the two configurations conflict with each other, the AP may be re-connected to the AC only based on the configurations on the AC.
- The fit AP configuration commands are automatically saved.

Configuration Steps

Configuring the Static IP Address of the AP

- Optional.
- When IP addresses of APs must be statically planned at the early stage of deployment, you can configure IP addresses on the APs.
- Configure the static IPv4 address of the AP so that the AP can use the IPv4 address to access the AC.

- Run the **apip ipv4** command to configure the static IPv4 address of the AP.

Command	**apip ipv4** *ip-addressnetwork-mask gateway*
Parameter Description	*ip-address*: indicates the static IP address. *network-mask*: indicates the subnet mask. *gateway*: indicates the gateway address.
Defaults	N/A
Command Mode	Global configuration mode on the AP
Usage Guide	N/A

Configuring the Static IP Address of the AC Accessed by the AP

- Optional.
- When the AP is configured to use the static IP address, you must also specify the IP address of the accessed AC on the AP.
- The static address type of the AC accessed by the AP must be the same as that of the AP. Ensure that both the AC and the AP use the IPv4 static address.
- Run the **acip ipv4** command so that the AP joins a specified IPv4 AC.

Command	**acipipv4** *ip-address* [*ip-address*…]
Parameter Description	*ip-address*: indicates the static IP address. At most six static addresses can be configured.
Defaults	N/A
Command Mode	Global configuration mode on the AP or AP configuration mode on the AC
Usage Guide	N/A

Enabling the AP to Use the PPPoE Dial-up Mode to obtain the Address

- Optional.
- When the AP needs to connect to a remote Internet service provider (ISP) through the ADSL and obtains the network access capability, run this command so that the AP can use the PPPoE dial-up mode to obtain the address.

Command	**apip pppoe**
Parameter Description	N/A
Defaults	By default, the PPPoE mode is not specified and the AP obtains the address through DHCP.
Command Mode	Global configuration mode on the AP
Usage Guide	The command configures only the mode (PPPoE dial-up mode) selected by the AP to obtain the address. After this command is configured, you need to add the PPPoE configurations and let the default route to point to the dialer

	interface so that the AP can communicate with the AC. CAPWAP can only select dialer 1 as the source interface. Therefore, when configuring the PPPoE dial-up mode, dialer 1 must be used.

Verification

- Check whether the fit AP configuration commands exist.
- Check whether the AP can communicate with the AC.

Configuration Example

Configuring the Static IP Address of the AC Accessed by the AP

Configuration Steps	• Configure the static IPv4 address of the AP. • Configure the static IPv4 address of the AC accessed by the AP.
AP	FS(config)# apip 192.168.1.2 255.255.255.0 192.168.1.1 FS(config)# acip ipv4 1.1.1.1
Verification	• Run the **show running-config** command to display the configurations.
AP	! apip 192.168.1.2 255.255.255.0 192.168.1.1 acip ipv4 1.1.1.1 !

Enabling the AP to Use the PPPoE Dial-up Mode to Obtain the Address

Configuration Steps	• Enable the AP to select the PPPoE dial-up mode to obtain the address. • Configure the PPPoE. • Configure the default route. • Configure the static IPv4 address of the AC accessed by the AP.

AP	FS(config)# apip pppoe FS(config)# interface FastEthernet 0/1 FS(config-if-FastEthernet 0/1)#pppoe enable FS(config-if-FastEthernet 0/1)#pppoe-client dial-pool-number 1 no-ddr FS(config-if-FastEthernet 0/1)#exit FS(config)# interfacedialer 1 FS(config-if-Dialer1)#ip address negotiate FS(config-if-Dialer1)#ppp chap hostname FS FS(config-if-Dialer1)#ppp chap password FS FS(config-if-Dialer1)#ppp pap sent-username FS password FS FS(config-if-Dialer1)#dialer pool 1 FS(config-if-Dialer1)#exit FS(config)#ip route 0.0.0.0 0.0.0.0 dialer 1 FS(config)# acip ipv4 1.1.1.1
Verification	● Run the **show running-config** command to display the configurations.
AP	! apip 192.168.1.2 255.255.255.0 192.168.1.1 acip ipv4 1.1.1.1 !

Common Errors

- N/A

3.4.12 Configuring AP Upgrade

Configuration Effect

- Upgrade the AP software version through configuration on the AC.

Notes

- Configure the data to activate the AP software version file. This command loads the **.bin** file to the memory only when the AP needs to be upgraded. When no AP needs to be upgraded, the bin file will be automatically removed from the memory.
- During the adaptive upgrade, the transitional version between FSOS10 and FSOS11 cannot be used to upgrade an AP using the FSOS10 system.
- When the bandwidth is limited, use the bandwidth control function for the upgrade.

Configuration Steps

Creating the AP Product Series

- (Optional) Run the **ap-serial** command to configure an AP product series on the AC.
- To upgrade the AP software version through the AC, you must configure the AP hardware version and product models for a specified product series on the AC.
- An AP software version is applicable to a series of AP products. You can configure the AP hardware version and product models for a specified product series, and use the software version to upgrade specified AP models.

Command	**ap-serial***serial-name ap-pid1 ap-pid2 ... ap-pidn* [**hw-ver** *hardware-version*]
Parameter Description	*serial-name*: indicates the name of the AP series to be created. *ap-pid1 ap-pid2 ... ap-pidn*: lists the product models to be added to the AP series. *hardware-version*: specifies the AP hardware version.
Defaults	No AP series is configured by default.
Command Mode	AC configuration mode
Usage Guide	N/A

Activating the AP Software Version File

- (Optional) Run the **active-bin-file** command to activate an AP software version on the AC.
- To upgrade the AP software version through the AC, you must activate the AP software version on the AC.
- Only an activated AP software version can be used for the upgrade.

Command	**active-bin-file** *filename*[**FSOS10**]
Parameter Description	*filename*: specifies the name of a software version. The name may contain a path prefix (**flash:**,**tmp:**, or**usb0:**), followed by a real file name. The maximum length of a file name is 64 bytes. **FSOS10:** indicates that a transitional version between 10.X and 11.X is activated. It is applicable only to the AP software version.
Defaults	The AP software version is not activated by default.
Command Mode	AC configuration mode
Usage Guide	1. To download a software version from the AC to upgrade an AP, you must first activate the version file. The FSOS10 system differs a lot from the FSOS11 system. Therefore, when using a transitional version between FSOS10 and FSOS11 for the upgrade, you must add the FSOS10 keyword. 2. The **.bin** file is loaded to the memory only when an AP needs to be upgraded. When no AP needs to be upgraded, the bin file will be automatically removed from the memory. 3. Before configuring this command, ensure that the software version file already exists in the AC system files.

Upgrading the Version of Specified APs

- Optional: Run the **ap-image** command to use a specified file to upgrade a specified AP series on the AC. This command takes effect on all APs connected to the AC.
- To upgrade the AP software version through the AC, you must first specify the upgrade file used by the AP.
- To upgrade a specified AP series, you must activate the AP software version, specify the AP series, and specify a file for upgrading the specified AP series.

Command	**ap-image** *filename*
Parameter	*filename*: specifies the software version name.

Description	
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	N/A

Configuring Adaptive Upgrade

- (Optional) Run the **ap-image auto-upgrade** command so that the AC can automatically identify applicable AP products based on the AP upgrade file and upgrade all applicable APs.
- The command automatically matches the AP models to which the software version is applicable and upgrades these APs.

Command	**ap-image**{ **auto-upgrade** | *filename serial-name*}
Parameter Description	**auto-upgrade:** indicates that the product model is automatically matched for the upgrade. *filename*: specifies the software version name. This file name must be the same as that specified by the **active-bin-file** command. *serial-name*: indicates the name of the AP series to be upgraded.
Defaults	N/A
Command Mode	AC configuration mode
Usage Guide	You can use the **auto-upgrade** option to automatically match the software version and upgrade APs without configuring the mapping relationship between the AP product models and software version. You can also use a specified file to upgrade a specified AP product series. When both the automatic upgrade mode and the specified series upgrade mode exist, the specified series upgrade mode is used preferentially. To enable the AC to upgrade the version of a specified AP product series, you must create the AP product series, configure the software version corresponding to the specified APs, and activate the software version. The three steps are mandatory.

Configuring the Maximum Number of APs That Can Be Concurrently Upgraded by the AC

- Optional.
- Limit the maximum number of APs that can be concurrently upgraded by the AC.

Command	**capwapupgrade max-concurrent** *num*
Parameter Description	*num*: indicates the maximum number of APs that can be concurrently upgraded by the AC. The default value is 18. The value ranges from 1 to 200.
Defaults	15
Command Mode	AC configuration mode
Usage Guide	N/A

Creating an Upgrade Group

- Optional.
- Create an upgrade group. The AC can evenly distribute the centralized upgrade quota to the upgrade group through balanced scheduling to limit the bandwidth and avoid wasting the bandwidth.

Command	**capwap upgrade group** *group-name* [**max-concurrent***num*]
Parameter	*group-name*: indicates the name of an upgrade group. The upgrade group name cannot be set to "default".

Description	*num*: indicates maximum number of APs that can be concurrently upgraded in the group. The default value is 5. The value ranges from 1 to 200.
Defaults	By default, no upgrade group is configured, and the AP upgrade is not limited by the bandwidth. When configuring an upgrade group, the maximum number of APs that can be concurrently upgraded in the group is 5 by default.
Command Mode	AC configuration mode
Usage Guide	N/A

Adding APs to an Upgrade Group

- Optional.
- Add APs to an upgrade group. Limit the number of APs that are upgraded in a centralized manner in this group through scheduling and configuration to control the bandwidth by upgrade group.

Command	**ap-upgrade group** *group-name*
Parameter Description	*group-name*: indicates the name of the upgrade group. Before adding APs to an upgrade group, you must run the **capwap upgrade group** command to create the upgrade group.
Defaults	APs are not added to any upgrade group.
Command Mode	AP configuration mode
Usage Guide	N/A

Configuring the Bandwidth Used for AP Upgrade

- Optional.
- Configure the bandwidth used for AP upgrade.

Command	**ap-upgrade band-width***num*
Parameter Description	*num*: indicates the bandwidth used for AP upgrade. The unit is 1 KB. The value ranges from 8 to 1024.
Defaults	The bandwidth is not limited.
Command Mode	AP configuration mode
Usage Guide	The bandwidth-limited AP upgrade configuration commands include the command for configuring the bandwidth used for AP upgrade, the command for creating an upgrade group, and the command for adding APs to the upgrade group.

Verification

- Check whether the AP version is successfully upgraded.
- Check the upgrade status of the bandwidth control upgrade group and APs in the group.

Configuration Example

Configuring the AP Upgrade Data

Configuration Steps	● Enter the AC configuration mode on the AC. ● Create the name of an AP product series on the AC. ● Activate the specified AP software version used for the upgrade on the AC. ● Configure the AP upgrade version file on the AC.
AC	FS(config-ac)# ap-serial serial1 AP220-E AP220-SE AP620-H hw-ver 1.0 FS(config-ac)# active-bin-file ap.bin FS(config-ac)# ap-image ap.bin serial1 FS(config-ac)# exit
Verification	● Display the list of files activated on the AC.
AC	FS#show ac-config active-file Cnt File Name Version Used Cnt Ready ------ ------------ ---------- ---------- -------- 1 ap.bin FSOS 10.4(1t7)(1T7), Release(88888) 1 1

Configuring the AP Upgrade During Which the Bandwidth is Under Control

Configuration Steps	● Enter the AC configuration mode on the AC. ● Create an AP upgrade group on the AC. ● Exit from the AC configuration mode. ● Enter the AP configuration mode. ● Configure the specified AP upgrade group on the AC. ● Activate the bandwidth used for AP upgrade on the AC.
AC	FS(config-ac)# capwap upgrade group UPGRADE-GROUP1 max-concurrent 10 FS(config-ac)# exit FS(config)#ap-config 8832.0000.1111 FS(config-ap)# ap-upgrade group UPGRADE-GROUP1 FS(config-ap)# ap-upgrade band-width 128 FS(config-ap)# exit
Verification	● Display the upgrade group and APs in the group on the AC. ● Display the APs and their bandwidths in an upgrade group on the AC.

AC	FS#show ac-config upgrade-group Cnt Group-Name Max-Concurrent Token cnt Upgrading cnt ------ ---------- ---------- 1 UPGRADE-GROUP1 10 2 1 FS#show ac-config upgrade-groupUPGRADE-GROUP1 Group have 2 ap, online 1 offline 1 Cnt Ap-Name Ap-Mac Online Upgrade Band-width ------- ---------- ---------- ------- ---------- --------- 1 ap220e 8832.0000.1111 true true 128 2 ap330 - false false 128 FS#show ap-config wtp-info 8832.0000.1111 FS#show ap-config wtp-info ap220e Upgrade-banfwidth : 128 Upgrade group : UPGRADE-GROUP1

Common Errors

- The AP upgrade data is configured, but the software version file used for the upgrade does not exist in the AC system files.

3.4.13 Configuring the CAPWAP Address Control

Configuration Effect

- Configure the maximum number of APs that can concurrently go online.

Notes

- If the configured value is too small, the total online duration of all APs connected to the AC will be relatively long.

Configuration Steps

Configuring the Maximum Number of APs That Can Concurrently Go Online

- Optional.
- On the AC, configure the maximum number of APs that can concurrently go online to prevent an excessively high CPU usage caused by a large number of CAPWAP control packets.

Command	**capwap max-concurrent** *num*
Parameter Description	*num*: indicates the maximum number of APs that can concurrently go online. The number ranges from 1 to 200.
Defaults	50
Command Mode	AC configuration mode

Usage Guide	If a large number of APs go online concurrently, the CPU usage of the AC may increase or even reach 100%. Consequently, tunnels of APs that are already online will be disconnected due to keepalive failures. You can use this command to limit the maximum number of APs go online concurrently.

Configuring the Number of CAPWAP Discovery Packets That Can Be Processed by an AC

- Optional.
- Configure the maximum number of discovery packets that can be processed by an AC on the AC to prevent exceedingly high CPU usage caused by considerable CAPWAP control packets.
- Run the ***capwap disc-concurrent*** *num* command to configure the number of discovery packets that can be processed.

Command	**capwap disc-concurrent** *num*
Parameter Description	The number of discovery packets that can be processed per second depends on the product capacity.
Defaults	The default value varies with the capacity value, for example, the default value is **256** for the WS7800.
Command Mode	AC global configuration mode
Usage Guide	The CAPWAP module needs to restrict the discovery packet processing concurrency based on the AC capacity, to prevent discovery packet attacks.

Verification

- Run the **show running-config** command to display the configurations.

Configuration Example

Configuring the Maximum Number of APs That Can Concurrently Go Online

Configuration Steps	• On the AC, configure the maximum number of APs that can concurrently go online.
AC	FS(config-ac)#capwap max-concurrent 100
Verification	• On the AC, run the **show running-config** command to display the configurations.
AC	! ac-controller capwap max-concurrent 100 !

Common Errors

- N/A

3.4.14 Configuring CAPWAP Fragmentation

Configuration Effect

- After a packet is encapsulated on the CAPWAP tunnel, the packet length may exceed the IP MTU, and will be fragmented at the IP layer. When the IP MTUs of multiple nodes on the link are inconsistent, the packet may be fragmented and reassembled for several times,

which reduces the packet forwarding performance. After CAPWAP fragmentation is enabled, the packet will be fragmented when encapsulated on the CAPWAP channel. The CAPWAP packet length is specified as the minimum IP MTU on the link, thereby avoiding fragmentation at the IP layer.

Notes

- If the configured MTU is too small, a lot of fragmented packets will be generated, affecting the packet forwarding performance. Even worse, large packets may fail to be transmitted. Therefore, it is important to determine the size of the MTU.
- The configured CAPWAP MTU must be equal to or smaller than the IP MTU at the egress of the device; otherwise, IP fragmentation will be performed after CAPWAP fragment.

Configuration Steps

Configuring the Path MTU of the CAPWAP Tunnel

- (Optional) Enter the AP or AP group configuration mode, and run the **capwap mtu** command to configure the path MTU of the CAPWAP tunnel.
- If the length of the packet encapsulated on the CAPWAP tunnel exceeds the path MTU of the CAPWAP tunnel, the packet will be fragmented on the CAPWAP tunnel. When configuring the path MTU of the CAPWAP tunnel on the AC, this path MTU must be set to the minimum IP MTU on the tunnel; otherwise, IP fragmentation and reassembly are performed again during packet forwarding, reducing the forwarding performance.

Command	**capwap mtu** *num*
Parameter Description	*num*: indicates the path MTU of the CAPWAP tunnel. The value ranges from 68 to 1500. The unit is byte.
Defaults	The default size of the MTU is 1500 bytes.
Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	N/A

Enabling CAPWAP Fragmentation

- Optional.
- When multiple IP MTU nodes exist on the transmission network, it is recommended that CAPWAP fragmentation be enabled on the AC, and the CAPWAP MTU be set to the path MTU.
- After a packet is encapsulated on the CAPWAP tunnel, the packet length may exceed the IP MTU, and will be fragmented at the IP layer. When the IP MTUs of multiple nodes on the link are inconsistent, the packet may be fragmented and reassembled for several times, which reduces the packet forwarding performance. You can run this command to enable CAPWAP fragmentation. After this function is enabled, the packet will be fragmented when encapsulated on the CAPWAP channel. The CAPWAP packet length can be specified in the **capwap mtu** command as the minimum IP MTU on the link, thereby avoiding fragmentation at the IP layer.

Command	**capwap fragment enable**
Parameter Description	N/A
Defaults	CAPWAP fragmentation is disabled by default.
Command Mode	AP configuration mode or AP group configuration mode

Usage Guide	N/A

Verification

- Check the detailed information about the CAPWAP to learn the MTU of the CAPWAP tunnel and whether the fragmentation function is enabled.
- Alternatively, run the **show ap-config running** command to check whether CAPWAP fragmentation is configured.

Configuration Example

Configuring the MTU of AP1 and Enabling the Fragmentation Function

Configuration Steps	• Set the path MTU of AP1 to 1200 bytes on the AC. • Enable CAPWAP fragmentation of AP1 on the AC.
AC	FS(config)# ap-config AP1 FS(config-ap)# capwap mtu 1200 FS(config-ap)# capwap fragment enable
Verification	Use the **show ap-config running** command to display the configurations.
AC	! capwap fragment enable capwap mtu 1200 !

Common Errors

- N/A

3.4.15 Configuring CAPWAP Encryption

Configuration Effect

- Disable the encryption function on the CAPWAP control channel to analyze packets when the network is faulty.

Notes

N/A

Configuration Steps

Configuring the Encryption Function on the CAPWAP Control Channel

- Optional.
- On the AC, you can disable the encryption function on the CAPWAP control channel to analyze packets for troubleshooting purpose when the network is faulty.

Command	**capwap dtls enable**
Parameter Description	N/A

Defaults	By default, the DTLS encryption function is enabled on the CAPWAP control channel.
Command Mode	AC configuration mode
Usage Guide	By default, the DTLS encryption function is enabled on the CAPWAP control channel to ensure security of interaction between the AC and the AP. In special cases, you can disable the encryption function on the CAPWAP control channel to facilitate tests.

Verification

- Check the detailed information about the CAPWAP tunnel to determine the encryption policy of the control channel and the data channel.
- Run the **show running-config** command to check whether encryption is enabled on the control channel.

3.4.16 Configuring CAPWAP Access Control

Configuration Effect

- Configure the maximum number of APs that can concurrently go online.

Notes

- If the configured value is too small, the total online duration of all APs connected to the AC will be relatively long.

Configuration Steps

Configuring the Maximum Number of APs That Can Concurrently Go Online

- Optional.
- On the AC, configure the maximum number of APs that can concurrently go online to prevent an excessively high CPU usage caused by a large number of CAPWAP control packets.

Command	**capwap max-concurrent** *num*
Parameter Description	*num*: indicates the maximum number of APs that can concurrently go online. The number ranges from 1 to 200.
Defaults	50
Command Mode	AC configuration mode
Usage Guide	If a large number of APs go online concurrently, the CPU usage of the AC may increase or even reach 100%. Consequently, tunnels of APs that are already online will be disconnected due to keepalive failures. You can use this command to limit the maximum number of APs go online concurrently.

Verification

- Run the **show running-config** command to display the configurations.

Configuration Example

Configuring the Maximum Number of APs That Can Concurrently Go Online

Configuration Steps	• On the AC, configure the maximum number of APs that can concurrently go online.

AC	FS(config-ac)#capwap max-concurrent 100
Verification	● On the AC, run the **show running-config** command to display the configurations.
AC	! ac-controller capwap max-concurrent 100 !

Common Errors

- N/A

3.4.17 Configuring the Echo Interval of the CAPWAP Tunnel

Configuration Effect

- (Optional) Configure the interval at which a keepalive packet is set.

Notes

- During deployment of the wireless network, the echo interval of the CAPWAP tunnel can be adjusted according to the network scale to properly plan the network convergence performance. During the adjustment, ensure that you have a good understanding about the network scale and confirm that the convergence is necessary. If a low echo interval is configured on a wireless network where a large number of APs are deployed, the network environment will be affected.

Configuration Steps

- (Optional) Enter the AP or AP group configuration mode for configuration.
- Configure the echo interval of the CAPWAP tunnel on the AC to control the keepalive period of the CAPWAP tunnel.

Command	**echo-interval** *seconds*
Parameter Description	*seconds*: indicates the echo interval of the CAPWAP tunnel. The value ranges from 5 to 255.
Defaults	30s
Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	In a fit AP network structure, an AC is interconnected with an AP through the CAPWAP tunnel. The Echo Request and Echo Response packets are used between the AP and the AC to maintain the effectiveness of links. If other request packets are not transmitted, the AP sends an Echo Request packet to the AC at the interval specified by **echo-interval** to keep the CAPWAP tunnel alive. If the AP does not receive any Echo Response packet, the Echo Request packet will be retransmitted. The transmission interval starts at the initial transmission interval (3s or half of **echo-interval**, whichever the smaller), and then is doubled upon next retransmission. The maximum retransmission interval cannot exceed the half of **echo-interval** or 60s, whichever the smaller. If the AP does not receive the Echo Response packet when **max-retransmit** (the maximum retransmission times) is reached, it is determined that the CAPWAP tunnel is disconnected. That is, the keepalive failure time of the tunnel is equal to the keepalive time plus the retransmission interval. This command takes effect only when the tunnel is in Run state. By default, **echo-interval** is 30s, and

	max-retransmit is 5. If the Echo Response packet is not received 0s after the Echo Request packet is sent, the Echo Request packet will be retransmitted at the interval of 3s, 6s, 12s, 15s, and 15s, respectively. The same rule is observed to calculate the packet timeout time if **echo-interval** and **max-retransmit** are set to other values.

Verification

- Check the detailed information about the CAPWAP tunnel. The modified interval at which the keepalive packet is sent should be displayed.

Configuration Example

Configuring the Echo Interval of the CAPWAP Tunnel

Configuration Steps	● On the AC, set the echo interval of the CAPWAP tunnel to 50s.
AC	FS(config)#ap-config AP0001 FS(config-ap)# echo-interval 50
Verification	● On the AC, check the detailed information about the CAPWAP tunnel.
AC	FS#show capwap 1.1.1.1 detail Echo interval is 50 secs, Dead interval is 119 secs

Common Errors

- N/A

3.4.18 Configuring the Maximum Retransmission Times of a CAPWAP Packet

Configuration Effect

- (Optional) Configure the maximum transmission times of a CAPWAP packet to adjust the keepalive time of the CAPWAP tunnel.

Notes

N/A

Configuration Steps

- (Optional) Enter the AP or AP group configuration mode for configuration.
- Configure the maximum transmission times of a CAPWAP packet to adjust the keepalive time of the CAPWAP tunnel.

Command	**capwap max-retransmit***num*
Parameter Description	*num*: indicates the maximum retransmission times of a CAPWAP packet
Defaults	5
Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	If the AP does not receive any Echo Response packet after sending an Echo Request packet, the Echo Request packet will be retransmitted. The transmission interval starts at the initial transmission interval (3s or half of **echo-interval**, whichever the smaller), and then is doubled upon next retransmission. The maximum retransmission interval cannot

	exceed the half of **echo-interval** or 60s, whichever the smaller. If the AP does not receive the Echo Response packet when **max-retransmit** (the maximum retransmission times) is reached, it is determined that the CAPWAP tunnel is disconnected. You can configure the maximum transmission times of a CAPWAP packet to adjust the keepalive time of the CAPWAP tunnel. This command takes effect only when the tunnel is in Run state.

Verification

- Check the detailed information about the CAPWAP tunnel. The modified interval at which the keepalive packet is sent should be displayed.

Configuration Example

Configuring the Maximum Retransmission Times of a CAPWAP Packet

Configuration Steps	● Set the maximum retransmission times of AP1 to 20.
AC	FS(config)#ap-config AP1 FS(config-ap)# capwap max-retransmit 20
Verification	● On the AC, check the detailed information about the CAPWAP tunnel.
AC	FS#show capwap 1.1.1.1 detail Config maxretransmit 20

Common Errors

- N/A

3.5 Monitoring

Displaying

Description	Command
Displays the list of files activated on the AC.	**show ac-config active-file**
Displays the mapping between AP product series configured on the AC and product models, and files used to upgrade the product series.	**show ac-config serial-product**
Displays the information about the upgrade group configured on the AC.	show ac-config upgrade-group [*group-name*]
Displays the data on the master board of the AP.	**show ap-config board-data** *ap-name*
Displays the status of links between ACs and APs.	**show ap-config link-latency** { **all** | **single** *ap-name* }
Displays the AP vendor information.	**show ap-config inventory** *ap-name*
Displays the AP restart statistics	**show ap-config reboot** *ap-name*
Displays the static IP address of an AP	**show ap-config static-ip**{ **all** | **single** *ap-name* }

Description	Command
Displays the AP location information	**show ap-config summary location**
Displays the AP upgrade status	**show ap-config updating-list**
Displays the AP status descriptions	**show ap-config wtp-descriptor** *ap-name*
Displays the AP status information	**show ap-config wtp-info** *ap-name*
Displays the detailed information about the CAPWAP tunnel	**show capwap** [index | [ip-address [port]]] **detail**
Displays the status of the CAPWAP tunnel	**show capwap state**
Displays the CAPWAP tunnel statistics	**show capwap** [index | [ip-address [port]]] **statistics**
Displays the AP version information	**show version** { **all** | *ap-name* }
Collects and displays various logs on an AP	**tran-data-start** *ap-name* {**exception** | **memory** | **tech-support** | **tech-package**} **tran-data-show** *ap-name* {**exception** | **cpuinfo** | **memory** | **syslog**| **tech-support**}

4 Configuring WBS

4.1 Overview

The Wireless Basic Service (WBS) is used to configure wireless-specific parameters on access controllers (ACs) when thin access points (APs) are deployed.

Link integrity detection is a basic service of the WBS. It detects the wired uplinks on APs. When the links are disconnected, the access services of the APs are stopped to force users offline. When the links are restored, the APs continue to provide wireless access services. Enabling link integrity detection in a fit AP architecture with dense AP deployment helps reduce the network disconnection time and improve user experience.

Protocols and Standards

- 802.11n: Enhancements for Higher Throughput

4.2 Applications

Application	Description
Configuring Fit APs	Run commands on ACs to configure the parameters of fit APs.
Enabling Link Integrity Detection	Enable link integrity detection in a fit AP architecture to improve the quality of service (QoS) of wireless access.

4.2.1 Configuring Fit APs

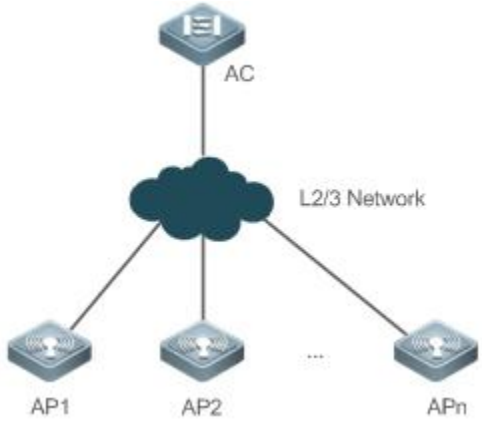
Scenario

Configure fit APs. Administrators can manage the configurations of fit APs on an AC in a centralized manner. Assume that a network has the following deployment requirements:

3. Allow the AC to monitor the status of the feeder links on i-Share APs.
4. Prevent stations (STAs) with received signal strength indication (RSSI) smaller than 20 from accessing the network.
5. Enable short guard interval (GI) in 20 MHz.
6. Prevent the use of low data rates, such as 1 Mbps, 2 Mbps, and 5.5 Mbps.

Figure 4-1 shows the fit AP networking topology.

Figure 4-1 Fit AP Networking Topology



Deployment

Main configuration points on the AC:

5. Enable i-Share antenna feeder link detection for all the APs and set the detection interval to an expected value.
6. Run **response-rssi** for the radios of all the APs and set the threshold to 20 dB.
7. Run **short-gi enable** for the radios of all the APs and set the bandwidth to 20 MHz.
8. Disable the use of the 1 Mbps, 2 Mbps, and 5.5 Mbps data rates for 802.11b/g network users.

4.2.2 Enabling Link Integrity Detection

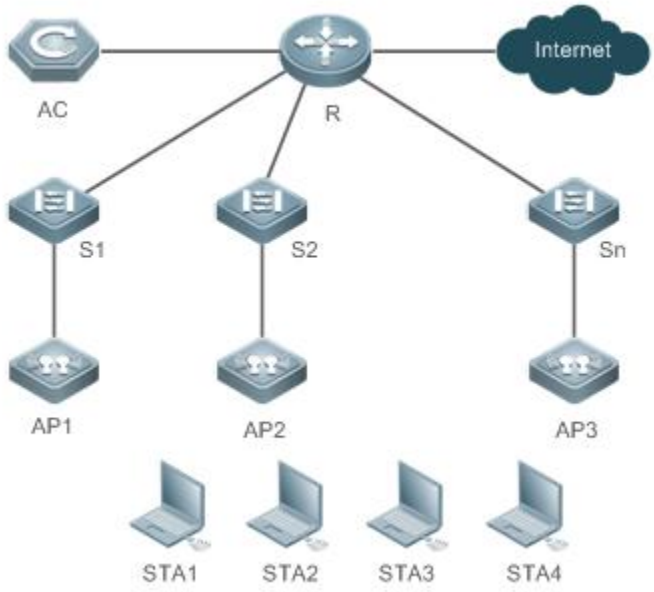
Scenario

Enable link integrity detection on wireless networks with a fit AP architecture.

See Figure 4-2.

- An AC is connected to the Internet through a router. AP1, AP2, and AP3 are connected to the router through three switches and associated with the AC.
- Station 1 (STA1) is associated with AP1, STA2 and STA3 are associated with AP2, and STA4 is associated with AP3. The STAs access the Internet through the AC.

Figure 4-2



Remarks	R is an egress router. S1, S2, and S3 are Layer-2 switches and function as the access devices for APs. AP1, AP2, and AP3 are directly connected to S1, S2, and S3.

Deployment

- Layer-2 switches provide the access service to APs.
- Router R sets up connections between ACs and APs and between STAs and the Internet.

4.3 Features

Basic Concepts

A-MPDU

The 802.11n standards adopt the aggregate MAC protocol data unit (A-MPDU). Multiple MPDUs are aggregated into an A-MPDU, and only one PHY header is retained whereas the PHY headers of other MPDUs are removed. In this way, the additional information of the PHY header of each MPDU to be transmitted is reduced, and the number of ACK frames is also reduced, which mitigates the burden and improves network throughput.

MCS

The physical layer of 802.11n supports high data transmission rates and is compatible with 802.11a/b/g rates. The many different speeds supported at the physical layer of 802.11n are called modulation and coding scheme (MCS) rates.

Beacon

The APs on wireless local area networks (WLANs) periodically send beacon frames externally. The beacon frames contain AP information. Wireless STAs receive beacon frames to discover WLANs.

RSSI

RSSI indicates the quality of wireless connections.

Country/Region Code

A country/region code identifies a country/region with radio frequency (RF) usage. RFs, channels, and powers vary with different country/region codes. Before you configure an AP, determine the country/region code that the AP supports. If the configured country/region code is changed, the RFs, channels, and powers mapped to the country/region code are also changed.

Frequency Band

FR transmission in the 2.4 GHz and 5 GHz frequency bands is supported.

Channel

Wireless channels transmit RF medium between APs and wireless STAs. The use of channels varies with different countries and frequency bands. In China, the 2.4 GHz frequency band can be configured with 13 channels (channel 1 to channel 13), and the 5 GHz frequency band can be configured with five channels (channels 149, 153, 157, 161, and 165). The overlapping channels in the 2.4 GHz frequency band generate interference. It is recommended that these channels be configured as non-overlapping channels (for example, channels 1, 6, and 11) to avoid radio signal collision. The five channels in the 5 GHz frequency band do not overlap or generate interference.

Transmit Power

Transmit power indicates the strength of the RF signals transmitted by an AP. It is proportional to the radio signal coverage area of the AP.

Timeslot Type

Channel contention may occur when multiple STAs send data on the same WLAN. To avoid this problem, STAs are required to check the idle state of channels before sending data. If an STA detects that a channel is idle, the STA does not send data until the backoff time has elapsed. The backoff time is a random integer of the slot time (which is an operation time unit specified in the Media Access Control [MAC] protocol). The value of the backoff time is automatically subtracted by 1 each time after the slot time has elapsed. When the

backoff time is reduced to 0, the STA starts sending data. The slot time on WLANs is classified into 20 μs and 9 μs, with the later being called short slot time.

Antenna Transmit/Receive Types

You can configure some antennas on an RF card to transmit signals and the other antennas to receive signals.

Short GI

802.11n adds optional support for a 0.4 μs guard interval, compared to the standard 0.8 μs guard interval.

Fragmentation Threshold

To increase the transmission success rate, the IEEE 802.11 MAC protocol supports the fragmentation of packets before transmission. Packets are fragmented according to a threshold, which reduces the interference probability and saves bandwidth resources during retransmission.

RTS

To avoid channel conflicts and the resulting data transmission failures, the IEEE 802.11 MAC protocol provides a handshake protocol called Request To Send/Clear To Send (RTS/CTS). When STA A needs to send data to STA B, it first sends an RTS frame. STA B responds with a CTS frame if it permits STA A to send data. After receiving the CTS frame, STA A starts sending data. When multiple STAs send RTS frames to the same STA, only the STAs that receive CTS frames are permitted to send data. The STAs that do not receive CTS frames can resend RTS frames after a time because a channel conflict is considered to have occurred.

PHY Protection Modes

Frames can be transmitted in Greenfield mode or hybrid mode. The hybrid mode is intended to support compatibility with other physical layers, and the Greenfield mode is used to transmit physical layer headers at high speeds. A device which uses the high-throughput (HT) hybrid mode can transmit frames in 802.11a/b/g and 802.11n modes. Such a device first transmits a conventional format preamble, followed by an HT format preamble. The device must send a conventional CTS-to-Self or RTS/CTS frame before transmitting data. These protection mechanisms enable 802.11a/b/g devices, including those devices not connected to APs in HT hybrid mode to sense the busy state of channels.

Preamble Type

A preamble is a group of bits in a packet header, used to synchronize the transmission signals between the transmit end and receive end. You can configure the preamble type (long or short) that an AP supports. The data frames with long preambles take a longer time to transmit than the data frames with a short preamble.

U-APSD

802.11e introduces Wi-Fi multimedia power save (WMM-PS) to reduce the delay of the services with high real-time requirements during the power management process. WMM-PS adopts the Unscheduled Automatic Power Save Delivery (U-APSD) technology to disable the transmission of radio signals during most of the time, which extends the battery life. U-APSD is an enhancement of the 802.11 power saving mechanism.

Overview

Feature	Description

Feature	Description
Configuring i-Share Antenna Feeder Link Detection	Checks the status of the feeder links on i-Share APs.
Configuring STA Access Control	Controls the access of specified wireless STAs.
Configuring AP RF Parameters	Configures the RF parameters for APs or radios.
Configuring Data Rate Control Parameters	Configures the RF parameters of data rate control.
Configuring Power-Save Parameters	Sets the parameters of power saving.
Enabling Link Integrity Detection	Detects the integrity of links to improve the wireless service quality.
Configuring E-Bag Parameters	Provides a command to quickly configure E-bag network optimization in one-click mode, which improves user experience.
Configuring WLANs in One-Click Mode	Provides the one-click WLAN configuration feature to perform fast configuration on devices with zero configurations.

4.3.1 Configuring i-Share Antenna Feeder Link Detection

Working Principle

FS Networks provides feeder link detection to facilitate the management of many i-Share APs on a network. This function detects the working status of all the feeders connected to each i-Share AP. Any improper connection or artificial damage of a feeder can be detected and rectified timely.

4.3.2 Configuring STA Access Control

Working Principle

FS Networks provides wireless STA access control.

Wireless STAs search for APs through active scan and passive scan.

- Active scan: A wireless STA sends a Probe Request frame to request access to an AP, which will respond with a Probe Response frame.
- Passive scan: APs broadcast beacon frames periodically. Wireless STAs listen to beacon frames and initiate connections to APs.

To control the network coverage areas of APs and improve the transmission quality of radio signals, the following methods are used to limit the access of wireless STAs:

- Control the beacon frame broadcast ranges of APs to limit the access of long-distance wireless STAs.
- Control the minimum RSSI value applied to wireless STAs during the access process. The STAs which send request frames with RSSI smaller than the minimum value are denied access.
- Control the minimum RSSI value applied to wireless STAs during the data transmission process. The STAs which send data frames with RSSI smaller than the minimum value are forced offline. Then the STAs can roam to other APs with better radio signals.

4.3.3 Configuring AP RF Parameters

You can configure the RF parameters for APs and radios.

Working Principle

A-MPDU

The 802.11n standards adopt A-MPDU. Multiple MPDUs are aggregated into an A-MPDU, and only one PHY header is retained whereas the PHY headers of other MPDUs are removed. In this way, the additional information of the PHY header of each MPDU to be transmitted is reduced, and the number of ACK frames is also reduced, which mitigates the burden and improves network throughput.

MCS

In 802.11n, RF rates are configured by using the index values of the MCS, which is used to express the communication rates on WLANs. The MCS is a rate table. The table columns show the factors of concern that affect communication rates, and the table rows show the MCS indexes. Each MCS index maps a physical transmission rate which is determined by a group of parameters. For the description of all the MCS rate tables, see the *IEEE P802.11n D2.00*.

Wireless Channel

Wireless channels transmit RF medium between APs and wireless STAs. The use of channels varies with different countries and frequency bands. In China, the 2.4 GHz frequency band can be configured with 13 channels (channel 1 to channel 13), and the 5 GHz frequency band can be configured with 24 channels (channels 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, and 165). The overlapping channels in the 2.4 GHz frequency band generate interference. It is recommended that these channels be configured as non-overlapping channels (for example, channels 1, 6, and 11) to avoid radio signal collision. The 24 channels in the 5 GHz frequency band do not overlap or generate interference.

Packet Fragmentation

To increase the transmission success rate, the IEEE 802.11 MAC protocol supports the fragmentation of packets before transmission. Packets are fragmented according to a threshold, which reduces the interference probability and saves bandwidth resources during retransmission.

RTS/CTS

To avoid channel conflicts and the resulting data transmission failures, the IEEE 802.11 MAC protocol provides a handshake protocol called RTS/CTS. When STA A needs to send data to STA B, it first sends an RTS frame. STA B responds with a CTS frame if it permits STA A to send data. After receiving the CTS frame, STA A starts sending data. When multiple STAs send RTS frames to the same STA, only the STAs that receive CTS frames are permitted to send data. The STAs that do not receive CTS frames can resend RTS frames after a time because a channel conflict is considered to have occurred.

If each STA implements RTS/CTS handshake before sending data, many RTS frames will occupy channel bandwidths. To avoid this problem, you can configure an RTS threshold to specify the frame length of transmitted data. If an STA sends data with a frame length smaller than the RTS threshold, the STA will not implement RTS/CTS handshake.

Beacon

The APs on WLANs periodically send beacon frames externally. The beacon frames contain AP information. Wireless STAs receive beacon frames to discover WLANs.

Preamble Type

A preamble is a group of bits in a packet header, used to synchronize the transmission signals between the transmit end and receive end. You can configure the preamble type (long or short) that an AP supports. The data frames with long preambles take a longer time to transmit than the data frames with a short preamble.

Timeslot Type

Channel contention may occur when multiple STAs send data on the same WLAN. To avoid this problem, STAs are required to check the idle state of channels before sending data. If an STA detects that a channel is idle, the STA does not send data until the backoff time has elapsed. The backoff time is a random integer of the slot time (which is an operation time unit specified in the MAC protocol). Assume that the random integer is 3. The value of the backoff time is automatically subtracted by 1 each time after the slot time has elapsed. When the backoff time is reduced to 0, the STA starts sending data. Reducing the slot time can reduce the overall backoff time and increase network throughput.

- **Channel Bandwidth**

In 802.11n, two 20 MHz bandwidths are combined into a 40 MHz bandwidth, which can be used as two 20 MHz bandwidths. (One 20 MHz bandwidth is the primary bandwidth, and the other is the secondary bandwidth. Data can be received and transmitted by using the 40 MHz bandwidth or two individual 20 MHz bandwidths.) In this way, data rates are doubled and wireless network throughput is increased.

- **GI**

802.11n adds optional support for a 0.4 μs guard interval, compared to the standard 0.8 μs guard interval.

8

- **Country/Region Code**

A country/region code identifies a country/region with RF usage. RFs, channels, and powers vary with different country/region codes. Before you configure an AP, determine the country/region code that the AP supports. If the configured country/region code is changed, the RFs, channels, and powers mapped to the country/region code are also changed.

- **Antenna Transmit/Receive Types**

APs use different quantities of antennas for transmitting and receiving signals, which enables APs to use two or three spatial streams to transmit signals in 802.11n mode, thus improving data transmission performance.

- **Internal Antenna and External Antenna**

Internal antennas are integrated inside the enclosures of APs, and external antennas are connected to the reserved hardware interfaces of APs. External antennas achieve longer transmission distances than internal antennas with the same transmission power.

- **Maximum Distance of Radio Transmission Between AP Radios and the Peer End**

Radio signals are transmitted in space at the speed of light. The longer the distance of radio transmission between AP radios and the peer end, the longer time it takes to transmit radio packets in space and the longer the timeout time for APs to wait for ACK and CTS frames. The timeout time must be adjusted based on the distance of radio transmission between AP radios and the peer end; otherwise, radio data transmission will fail. A very long timeout time will cause resource waste on the air interface when APs are still waiting for ACK and CTS frames.

4.3.4 Configuring Data Rate Control Parameters

You can configure the RF parameters of data rate control.

Working Principle

802.11 is the industry standards that the Institute of Electrical and Electronics Engineers (IEEE) developed for WLAN communications. 802.11x is an improvement over 802.11. The main transmission standards include 802.11b, 802.11a, 802.11g, and 802.11n.

1. 802.11b

The operating band is 2.4 GHz, and the data transmission rate can reach 11 Mbps, which can be reduced to 5.5 Mbps, 2 Mbps, or 1 Mbps based on actual requirements.

2. 802.11a

The operating band is 5 GHz, and the data transmission rate can reach 54 Mbps, which can be reduced to 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 Mbps, or 6 Mbps based on actual requirements.

3. 802.11g

The operating band is 2.4 GHz, and the data transmission rate can reach 54 Mbps, which can be reduced to 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 Mbps, or 6 Mbps based on actual requirements. 802.11g STAs are backward compatible with 802.11b.

4.3.5 Configuring Power-Save Parameters

Working Principle

- DTIM Period

A delivery traffic indication map (DTIM) is a flag bit in a beacon frame, used to determine the interval at which an AP sends broadcast or multicast frames. APs buffer the data that wireless STAs in dormant state need to receive according to the DTIM period. After the DTIM period has elapsed, APs send the buffered data to wireless STAs.

The DTIM period is expressed based on the number of sent beacon frames. Assume that the DTIM period is set to 3. APs send broadcast or multicast frames each time after three beacon frames are sent.

- U-APSD Power Saving

U-APSD is an improvement over the power saving mode. When clients are associated with ACs, the clients can configure which ACs have the trigger attribute, which ACs have the delivery attribute, and the maximum number of packets to be sent after trigger. The trigger and delivery attributes can be modified when flows are created through connection access control (CAC). When a client sleeps, the delivery-enabled AC packets destined for the client are buffered. To retrieve the buffered packets, the client needs to send trigger-enabled AC packets. After receiving the trigger-enabled AC packets, the AP sends the buffered packets according to the to-be-sent packet quantity determined during the access process. Other AC packets than delivery-enabled AC packets are stored and transmitted in accordance with the 802.11 standards.

4.3.6 Enabling Link Integrity Detection

APs are wireless access devices without the switching feature. They implement all functions of the physical layer and partial functions of the MAC layer. A fat AP or fit AP has only one wired uplink, which is the data channel allowing STAs to access the AP. When the wired uplink is disconnected because of a fault, all the wireless STAs connected to the AP cannot access the Internet.

Wireless STAs cannot sense link disconnections immediately or take measures; as a result, the network connection cannot be restored for a long time.

Link integrity detection is designed to solve this problem.

Working Principle

The link integrity detection function continuously detects the status of the wired uplinks on APs. When a wired uplink is disconnected, the RF interface of the AP is disabled to stop the access service. The wireless STAs associated with the AP are forced offline and have to reconnect to other normal APs.

When the wired uplink is recovered, the link integrity detection function enables the RF interface of the AP again to restore the wireless access service.

Link integrity detection enables the wireless STAs that are associated with APs with disconnected wired uplinks to reconnect to other normal APs.

4.3.7 Configuring E-Bag Parameters

You can configure the E-bag parameters for APs and radios.

Working Principle

You can run a command to quickly configure E-bag network optimization in one-click mode, which improves user experience.

- **A-MPDU**

A-MPDU is short for aggregate MAC protocol data unit.

- **LDPC**

A low-density parity-check (LDPC) code is a linear error correcting code. Being easy to use and with low complexity, this coding method adopts the forward error correction (FEC) technology to improve the coding reliability and gains. LDPC was developed at the beginning of the 1960 and supports the transmission of information in noisy frequencies with massive background or content damage. It also greatly reduces the probability of information loss during transmission in frequencies with serious noise interference. However, a small number of STAs are not compatible with LDPC, and enabling LDPC will result in packet loss.

- **STBC**

Space time block coding (STBC) is a technique used in wireless communications to transmit multiple copies of a data stream across a number of antennas at different time points to improve the reliability of data transmission by means of time diversity and space diversity. The outstanding advantage of STBC is the use of maximum likelihood decoding to obtain complete antenna gains. Some STAs may not be compatible with STBC.

- **A-MPDU Software Retransmission Times**

The A-MPDU software retransmission mechanism is designed to avoid the loss of sub-frames in wireless communications. The greater the retransmission times, the lower the probability of sub-frame loss. If packets are retransmitted frequently, the burden on the air interface is increased, which affects the real-time transmission of packets on the air interface. You can increase the retransmission times if you need to avoid packet loss when there is a high probability of sub-frame loss.

- **A-MPDU-RTS**

The RTS protection feature of A-MPDU prevents resource waste on the air interface caused by packet collision due to hidden nodes. Because RTS interaction consumes air interface resources and has resulting adverse impact in many application scenarios, this feature is disabled by default. Enable RTS protection only when the resource waste on the air interface caused by hidden nodes is greater than the resource consumption of RTS interaction on the air interface.

- **Single-Time Received Ethernet Packet Quantity**

A command is provided to adjust the number of Ethernet packets received at a single time. Increasing Ethernet packet reception can improve network performance but may reduce APs' ability to handle key packets in real time. You can reduce Ethernet packet reception when the requirements for performance are not high but user concurrency and real-time packet handling are demanded. In this case, it is recommended that the single-time received Ethernet packet quantity be set to 25.

4.3.8 Configuring WLANs in One-Click Mode

The one-click WLAN configuration feature allows you to perform fast configuration on devices with zero configurations.

Working Principle

autowifi

Perform the following configuration on an AC:

3. Division of virtual local area networks (VLANs): On the AC, configure VLAN1 as the VLAN for APs and VLAN2 as the VLAN for STAs.

4. Address pool: On the AC, configure the 192.168.1.0 network segment as the address pool for APs and configure the 192.168.2.0 network segment as the network segment for STAs. The default IP addresses of VLAN1 and VLAN2 are 192.168.1.1 and 192.168.2.1 respectively. The default management IP address is 88.88.88.88.

5. WLAN configuration: Name the WLAN **autowifi_***XXXX*. The last four characters are the last four digits of the MAC address of the AC. You can use wlan-id 1.

6. Security: By default, WPA2 encryption is used. The password is **autowifi**.

7. WLAN-VLAN mapping: On the AC, configure the mapping between wlan-id 1 and VLAN2 in the group named **ap-group default**.

8. Service: Enable the Dynamic Host Configuration Protocol (DHCP) service.

4.4 Configuration

Configuration	Description and Command	
Configuring i-Share Antenna Feeder Link Detection	(Optional) It is used to enable feeder link detection for APs.	
	antdetect enable	Enables feeder link detection.
	antdetect interval	Configures the detection interval, in the unit of minutes.
Configuring STA Access Control	(Optional) It is used to configure STA access control.	
	{**802.11a** | **802.11b**} **network** {**enable** | **disable**}	Enables or disables the 2.4 GHz or 5 GHz network.
	11asupport enable	Enables 802.11a support for specified AP radios in 5 GHz.
	11bsupport enable	Enables 802.11b support for specified AP radios in 2.4 GHz.
	11gsupport enable	Enables 802.11g support for specified AP radios on the 2.4 GHz network.
	11nasupport enable	Enables 802.11n support for specified AP radios in 5 GHz.
	11ngsupport enable	Enables 802.11n support for specified AP radios in 2.4 GHz.
	11acsupport enable	Enables 802.11ac support for specified AP radios.
	coverage-area-control	Configures the management frame power for APs.

Configuration	Description and Command	
Configuring i-Share Antenna Feeder Link Detection	(Optional) It is used to enable feeder link detection for APs.	
	antdetect enable	Enables feeder link detection.
	antdetect interval	Configures the detection interval, in the unit of minutes.
	response-rssi	Configures the minimum RSSI for wireless STAs to connect to specified AP radios.
	assoc-rssi	Configures the minimum RSSI for wireless STAs to maintain connections to specified AP radios.
Configuring AP RF Parameters	(Optional) It is used to configure the RF parameters for APs.	
	802.11n a-mpdu enable	Enables A-MPDU for specified AP radios.
	802.11n mcs support	Configures the maximum 802.11n MCS index value for specified AP radios.
	802.11ac mcs support	Configures the maximum 802.11ac MCS index value for specified AP radios.
	antenna	Configures the antenna transmit/receive type for specified AP radios.
	external-antenna enable	Enables usage of external antennas for specified AP radios, and disables usage of internal antennas.
	beacon dtim-period	Configures the DTIM period for specified AP radios.
	beacon period	Configures the beacon frame transmission period for specified AP radios.
	chan-with	Configures bandwidth assignments for specified AP radios.
	channel	Configures channel assignments for specified AP radios.
	country	Configures the country/region code set supported by an AC or the country/region code used by AP radios.
	enable-radio	Enables specified or all AP radios.
	fragment-threshold	Configures the fragmentation threshold for specified AP radios.
	green-field enable	Enables the protection mode for specified AP radios.
	power local	Configures the transmit power for specified AP radios.
	radio-type	Specifies the operating band for specified AP radios.
	rts-threshold	Configures the RTS threshold for specified AP radios.

Configuration	Description and Command	
Configuring i-Share Antenna Feeder Link Detection	(Optional) It is used to enable feeder link detection for APs.	
	antdetect enable	Enables feeder link detection.
	antdetect interval	Configures the detection interval, in the unit of minutes.
	short-gi	Enables short GI for specified AP radios.
	update-key-tsc enable	Enables TKIP Sequence Counter (TSC) update for APs during 802.11x re-authentication.
	peer-distance	Configures the maximum distance of wireless transmission between APs and the peer end.
	mu-mimo enable	Configures MIMO for multi users.
Configuring Data Rate Control Parameters	(Optional) It is used to configure the parameters of data rate control.	
	802.11a network rate	Configures the data rate set supported by 802.11a STAs.
	802.11b network rate	Configures the data rate set supported by 802.11b STAs.
	802.11g network rate	Configures the data rate set supported by 802.11g STAs.
	mcast-rate	Configures the WLAN multicast rate.
	beacon rate	Configures the beacon frame transmission rate.
Configuring Power-Save Parameters	(Optional) It is used to configure the power-save parameters.	
	beacon dtim-period	Configures the DTIM period.
	apsd	Enables or disables U-APSD power saving.
Enabling Link Integrity Detection	(Mandatory) It is used to enable link integrity detection.	
	link-check enable	Enables link integrity detection.
Configuring E-Bag Parameters	(Optional) It is used to configure the parameters of E-bag.	
	ampdu-retries	Configures the A-MPDU software retransmission times.
	ampdu-rts	Enables or disables RTS protection for A-MPDU packets.
	eth-schd	Configures the single-time received Ethernet packet quantity for APs.
	ldpc	Enables or disables LDPC.
	stbc	Enables or disables transmit/receive STBC.
	ebag	Configures E-bag network optimization in one-click mode.
Configuring WLANs in One-Click Mode	(Optional) It is used to configure WLANs in one-click mode.	
	autowifi	Configures WLANs in one-click mode.

4.4.1 Configuring i-Share Antenna Feeder Link Detection

Configuration Effect

- Enable i-Share antenna feeder link detection to allow i-Share APs to periodically detect the status of antenna feeder links. When an antenna feeder link is abnormal, the i-Share AP uploads the abnormality information to an AC, and the network management personnel can locate the problem and rectify the fault in a timely manner.

Notes

- i-Share antenna feeder link detection is supported only by AP220-E(M) v3.0.

Configuration Steps

Enabling Feeder Link Detection

- Optional.
- On an AC, enable i-Share antenna feeder link detection for APs.
- The AC assigns the settings to the APs to instruct the APs to enable feeder link detection. When an AP detects feeder link abnormalities, it uploads abnormal state information to the AC, on which you can view the feeder link status.

Command	**antdetect enable**
Parameter Description	N/A
Defaults	By default, feeder link detection is disabled.
Command Mode	AP configuration mode
Configuration Usage Guide	By default, feeder link detection is disabled.

Configuring the Interval of Feeder Link Detection

- Optional.
- On an AC, enable feeder link detection for APs, and then configure the detection interval. The detection interval takes effect only after feeder link detection is enabled.
- The AC assigns the detection interval settings to the APs to instruct the APs to detect the feeder link status according to specified interval.

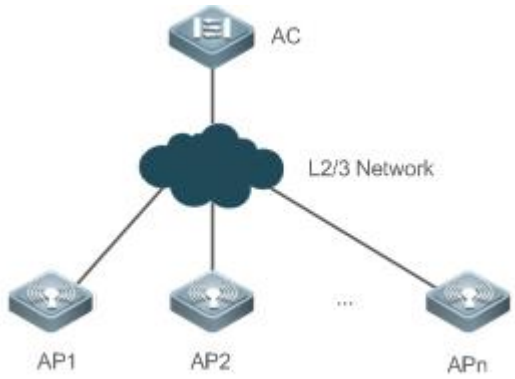
Command	**antdetect interval** *interval*
Parameter Description	*Interval*: specifies the interval at which the feeder link status is detected. The value ranges from 1 to 10000, in the unit of minutes.
Defaults	The default value is 1 minute, indicating that the feeder link status is detected every 1 minute.
Command Mode	AP configuration mode
Configuration Usage Guide	By default, the feeder link status is detected every 1 minute.

Verification

- Run **show antenna all** to display the status of the antenna feeder links of all APs.

Configuration Example

- **Enabling Feeder Link Detection**

Scenario **Figure 4- 3**	 In Figure 4- 3, an AC is connected to thin APs. Enable i-Share antenna feeder link detection on the AC according to the following steps: 1. Enable feeder link detection for all the APs. 2. Set the detection interval to 30 minutes.
Configuration Steps	● Enable i-Share antenna feeder link detection on the AC.
	FS# configure terminal FS(config)# ap-config all FS(config-ap)# antdetect enable FS(config-ap)# antdetect interval 30
Verification	● Run **show antenna all** to display the status of the antenna feeder links of all APs.
	FS# show antenna all ap's antenna state R1 R2 R3 R4 R5 R6 ap 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 ---------- ------- ------- ------- ------- ------- ------- APD-M4 - N N - - N Y - - N N - - N N - - - - - - - -

4.4.2 Configuring STA Access Control

Configuration Effect

- Control the access of a specified type of wireless STAs to manage these wireless STAs conveniently.

Configuration Steps

Enabling or Disabling the 2.4 GHz or 5 GHz Network

- Optional.
- Enable or disable the 2.4 GHz or 5 GHz network on an AC.
- The AC assigns the network settings to all the APs to instruct the APs to enable or disable the 2.4 GHz or 5 GHz network.

Command	{ **802.11a** | **802.11b**} **network** { **enable** | **disable** }
Parameter Description	N/A
Defaults	By default, the 2.4 GHz and 5 GHz networks are enabled.
Command Mode	AC configuration mode
Configuration Usage Guide	N/A

Enabling 802.11a Support

- Optional.
- The configuration takes effect only when the AP radios operate in 5 GHz.
- On the AC, enable 802.11a support for specified APs.
- The AC assigns the settings to the APs to instruct the APs to support the access of 802.11a STAs in 5 GHz.

Command	**11asupport enable radio** *radio-id*
Parameter Description	*radio-id*: specifies the IDs of the radios enabled with 802.11a support. The value ranges from 1 to 48.
Defaults	By default, the access of 802.11a STAs is supported in 5 GHz.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration takes effect only when the AP radios operate in 5 GHz. The configuration is supported only by certain APs.

Enabling 802.11b Support

- Optional.
- The configuration takes effect only when the AP radios operate in 2.4 GHz.
- On the AC, enable 802.11b support for specified APs.
- The AC assigns the settings to the APs to instruct the APs to support the access of 802.11b STAs in 2.4 GHz.

Command	**11bsupport enable radio** *radio-id*
Parameter	*radio-id*: specifies the IDs of the radios enabled with 802.11b support. The value ranges from 1 to 48.

Description	
Defaults	By default, the access of 802.11b STAs is supported in 2.4 GHz.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration takes effect only when the AP radios operate in 2.4 GHz. The configuration is supported only by certain APs.

Enabling 802.11g Support

- Optional.
- The configuration takes effect only when the AP radios operate in 2.4 GHz.
- On the AC, enable 802.11g support for specified APs.
- The AC assigns the settings to the APs to instruct the APs to support the access of 802.11g STAs in 2.4 GHz.

Command	**11gsupport enable radio** *radio-id*
Parameter Description	*radio-id*: specifies the IDs of the radios enabled with 802.11g support. The value ranges from 1 to 48.
Defaults	By default, the access of 802.11g STAs is supported in 2.4 GHz.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration takes effect only when the AP radios operate in 2.4 GHz. The configuration is supported only by certain APs.

Enabling 802.11na Support

- Optional.
- The configuration takes effect only when the AP radios operate in 5 GHz.
- On the AC, enable 802.11na support for specified APs.
- The AC assigns the settings to the APs to instruct the APs to support the access of 802.11n STAs in 5 GHz.

Command	**11nasupport enable radio** *radio-id*
Parameter Description	*radio-id*: specifies the IDs of the radios enabled with 802.11na support. The value ranges from 1 to 48.
Defaults	By default, the access of 802.11n STAs is supported in 5 GHz.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration takes effect only when the AP radios operate in 5 GHz. The configuration is supported only by certain APs.

Enabling 802.11ng Support

- Optional.
- The configuration takes effect only when the AP radios operate in 2.4 GHz.
- On the AC, enable 802.11ng support for specified APs.
- The AC assigns the settings to the APs to instruct the APs to support the access of 802.11n STAs in 2.4 GHz.

Command	**11ngsupport enable radio** *radio-id*
Parameter Description	*radio-id*: specifies the IDs of the radios enabled with 802.11ng support. The value ranges from 1 to 48.
Defaults	By default, the access of 802.11n STAs is supported in 2.4 GHz.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration takes effect only when the AP radios operate in 2.4 GHz. The configuration is supported only by certain APs.

Enabling 802.11ac

- Optional.
- On the AC, enable 802.11ac support for specified APs.
- The AC delivers configuration to the APs to instruct the APs to support the access of 802.11ac STAs.

Command	**11acsupport enable radio** *radio-id*
Parameter Description	*radio-id*: specifies the IDs of the radios enabled with 802.11ac support. The value ranges from 1 to 48.
Defaults	Only the radios with even IDs support the access of 802.11ac STAs.
Command Mode	AP configuration mode
Configuration Usage Guide	N/A

Configuring the Management Frame Power for APs

- Optional.
- Perform the configuration only on the required device unless otherwise specified.
- On the AC, configure the management frame power for specified APs.
- The AC assigns the settings to the APs to instruct the APs to use the configured management frame transmit power. In this way, the signal coverage areas of the APs are controlled to limit the access of wireless STAs.

Command	**coverage-area-control** *power*
Parameter Description	*power*: specifies the management frame power. The value ranges from 0 to 32, in the unit of dBm.
Defaults	By default, the management frame power for APs is 0 dBm.
Command Mode	AP configuration mode/AP group configuration mode
Configuration Usage Guide	N/A

Configuring the Minimum RSSI for Wireless STAs to Access APs

- Optional.
- On the AC, configure the minimum RSSI for wireless STAs to access specified AP.

- The AC assigns the settings to the APs to instruct the APs to use the configured minimum RSSI as the threshold for allowing the access of wireless STAs.

Command	**response-rssi** *rssi* **radio** { *radio-id* | [*802.11b* | *802.11a*] }
Parameter Description	*rssi:* specifies the minimum RSSI for wireless STAs to access APs. The value ranges from 0 to 100, in the unit of dB. *radio-id*: specifies the IDs of the radios assigned with the minimum RSSI. The value ranges from 1 to 48. *802.11b*: indicates that the minimum RSSI is assigned to all the radios in 2.4 GHz. *802.11a*: indicates that the minimum RSSI is assigned to all the radios in 5.8 GHz.
Defaults	By default, the RSSI is set to **0**, indicating that there is no RSSI limit on the access of wireless STAs.
Command Mode	AP configuration mode
Configuration Usage Guide	If you select **802.11b**, the minimum RSSI is configured for all the radios in 2.4 GHz. The settings take effect when the APs go online for the first time and are automatically applied to the radios. If you select **802.11a**, the condition is the same for the radios in 5.8 GHz.

Configuring the Minimum RSSI for Wireless STAs to Maintain Connections to APs

- Optional.
- On the AC, configure the minimum RSSI for wireless STAs to maintain connections to specified AP.
- The AC assigns the settings to the APs to instruct the APs to use the configured minimum RSSI as the threshold for maintaining the connections of wireless STAs.

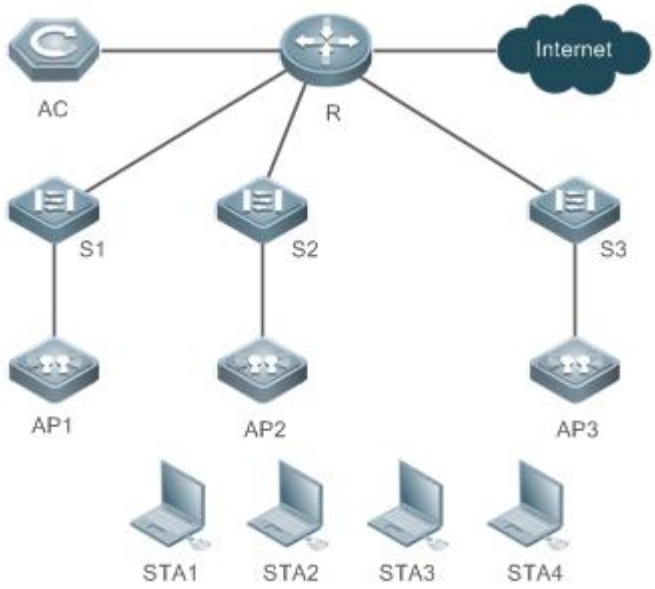
Command	**assoc-rssi** *rssi* **radio** *radio-id*
Parameter Description	*rssi:* specifies the minimum RSSI for wireless STAs to maintain connections. The value ranges from 0 to 100, in the unit of dB. *radio-id*: specifies the IDs of the radios assigned with the minimum RSSI. The value ranges from 1 to 48.
Defaults	By default, the RSSI is set to **0**, indicating that there is no RSSI limit on the access of wireless STAs.
Command Mode	AP configuration mode
Configuration Usage Guide	N/A

Verification

- Run **show ap-config running** *ap-name* to display the parameter settings of STA access control.

Configuration Example

Configuring the Parameters of STA Access Control

Scenario **Figure 4-4**	 In Figure 4-4, an AC is connected to fit APs. On the AC, configure STA access control for all the APs according to the following step: 1. Disable the 2.4 GHz network.
	On the AC, configure STA access control for AP1 according to the following steps: 1. Enable the access of 802.11a and 802.11na STAs in 5 GHz 2. Enable the access of 802.11g and 802.11ng STAs in 2.4 GHz. 3. Enable the access of 802.11ac STAs. 4. Set the management frame power to 20 dBm. 5. Set the minimum RSSI for wireless STAs to access APs to 20 dB. 6. Set the minimum RSSI for wireless STAs to maintain connections to15 dB.
Configuration Steps	● Disable the 2.4 GHz network on the AC.
AC	FS# configure terminal FS(config)# ac-controller FS(config-ac)# 802.11b network disable
	● Set the STA access control parameters for AP1 on the AC.
AC	FS# configure terminal FS(config)# ap-config AP1 FS(config-ap)# 11asupport enable radio 2 FS(config-ap)# 11nasupport enable radio 2 FS(config-ap)# 11gsupport enable radio 1

	FS(config-ap)# 11ngsupport enable radio 1 FS(config-ap)# 11acsupport enable radio 1 FS(config-ap)# no 11bsupport enable radio 1 FS(config-ap)# coverage-area-control 20 FS(config-ap)# response-rssi 20 radio 1 FS(config-ap)# response-rssi 20 radio 2 FS(config-ap)# assoc-rssi 15 radio 1 FS(config-ap)# assoc-rssi 15 radio 2
Verification	● Run **show running** to check whether the 2.4 GHz or 5 GHz network is enabled or disabled.

AC	FS(config)# show running
	!
	ac-controller
	  sta-limit 1024
	  no capwap dtls enable
	  802.11b network disable
	  country CN
	  country US
	!

	● Run **show ap-config running** *ap-name* to display the STA access control parameters for AP1.

AC	FS(config)# show ap-config running AP1
	!
	ap-config 220em
	no 11bsupport enable radio 1
	  coverage-area-control 20
	  response-rssi 20 radio 1
	  response-rssi 20 radio 2
	assoc-rssi 15 radio 1
	  assoc-rssi 15 radio 2
	  radio-type 1 802.11b
	  radio-type 2 802.11a
	!

4.4.3 Configuring AP RF Parameters

Configuration Effect

- Configure the RF parameters for APs and radios for easier configuration management.

Configuration Steps

Enabling A-MPDU

- Optional.
- On an AC, enable A-MPDU for specified APs. Then the AC delivers the configuration to the APs to instruct the APs to enable A-MPDU.

Command	**802.11n a-mpdu enable radio** *radio-id*
Parameter Description	*radio-id*: specifies the IDs of the radios enabled with A-MPDU. The value ranges from 1 to 48.
Defaults	By default, A-MPDU is enabled.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration takes effect only when the AP radios operate in 802.11n or 802.11ac mode. The configuration is supported only by certain APs.

Configuring the Maximum 802.11n MCS Index Value

- Optional.
- On an AC, configure the maximum 802.11n MCS index value for specified AP. Then the AC delivers the configuration to the APs to inform the APs of the maximum 802.11n MCS index value.

Command	**802.11n mcs support** *num* **radio** *radio-id*
Parameter Description	*num*: specifies the MCS index value, which ranges from 0 to 23. *radio-id*: specifies the IDs of the radios assigned with the maximum 802.11n MCS index value. The value ranges from 1 to 48.
Defaults	By default, the maximum 802.11n MCS index value is 23.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration takes effect only when the AP radios operate in 802.11n or 802.11ac mode.

Configuring the Maximum 802.11ac MCS Index Value

- Optional.
- On an AC, configure the maximum 802.11ac MCS index value for specified AP. Then the AC delivers the configuration to the APs to inform the APs of the maximum 802.11ac MCS index value.

Command	**802.11ac mcs support** *num* **radio** *radio-id*
Parameter Description	*num*: specifies the MCS index value, which ranges from 0 to 48. *radio-id*: specifies the IDs of the radios assigned with the maximum 802.11ac MCS index value. The value ranges from 1 to 48.

Defaults	By default, the maximum 802.11n MCS index value is 29.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration takes effect only when the AP radios operate in 802.11ac mode.

Configuring the Antenna Transmit/Receive Type

- Optional.
- On an AC, configure the antenna transmit/receive type for specified APs. Then the AC assigns the settings to the APs to instruct the APs to use the specified antenna selection masks to send and receive packets.

Command	**antenna** { **transmit** | **receive** } *value* **radio** *radio-id*
Parameter Description	**transmit**: is the antenna transmit parameter. **receive**: is the antenna receive parameter. *value*: specifies the antenna selection mask. The value ranges from 1 to 15. *radio-id*: specifies the IDs of the radios assigned with the antenna transmit/receive type. The value ranges from 1 to 48.
Defaults	In AP configuration mode, the default antenna selection mask varies with different product models and antenna quantities and is determined based on the product model. By default, no antenna transmit/receive type is configured in AP group configuration mode.
Command Mode	AP configuration mode or AP group configuration mode
Configuration Usage Guide	The configuration takes effect only when the AP radios operate in 802.11n or 802.11ac mode.

Configuring Usage of External Antennas for APs

- Optional.
- On an AC, configure usage of external antennas for specified APs. Then the AC assigns the settings to the APs to instruct the APs to enable external antennas and disable internal antennas.

Command	**external-antenna enable radio** *radio-id*
Parameter Description	*radio-id*: specifies the IDs of the radios enabled with external antenna usage. The value ranges from 1 to 48.
Defaults	By default, usage of internal antennas is enabled, and usage external antennas is disabled.
Command Mode	AP configuration mode
Configuration Usage Guide	N/A

Configuring the Beacon Frame Transmission Period

- Optional.
- On an AC, configure the beacon frame transmission period for specified APs. Then the AC assigns the settings to the APs to instruct the APs to transmit beacon frames according to the configured period.

Command	**beacon period** *milliseconds* **radio** *radio-id*

Parameter Description	*milliseconds*: specifies the beacon frame transmission period. The value ranges from 20 to 1000, in the unit of ms. *radio-id*: specifies the IDs of the radios assigned with the beacon frame transmission period. The value ranges from 1 to 48.
Defaults	By default, the beacon frame transmission period is 100 ms.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration is supported only by certain APs.

Configuring Bandwidth Assignments

- Optional.
- On an AC, configure bandwidth assignments for specified APs. Then the AC assigns the settings to the APs to instruct the APs to switch the channel bandwidth to the specified bandwidth.

Command	**chan-width** { **20** | **40** | **80** | **160** } **radio** {*radio-id* | [*802.11b* | *802.11a*]}
Parameter Description	**20**: specifies the 20 MHz bandwidth. **40**: specifies the 40 MHz bandwidth. **80**: specifies the 80 MHz bandwidth. **160**: Specifies the **160** MHz bandwidth. *radio-id*: specifies the IDs of the radios assigned with bandwidth. The value ranges from 1 to 48. **802.11b**: indicates that bandwidth is assigned to all the radios in 2.4 GHz. **802.11a**: indicates that bandwidth is assigned to all the radios in 5.8 GHz.
Defaults	The default channel bandwidth is 20 Mbps.
Command Mode	AP configuration mode
Configuration Usage Guide	If you select **802.11b**, the bandwidth is configured for all the radios in 2.4 GHz. The settings take effect when the APs go online for the first time and are automatically applied to the radios. If you select **802.11a**, the condition is the same for the radios in 5.8 GHz. The bandwidth configuration takes effect only when APs operate in 802.11n or 802.11ac mode.

Configuring Channel Assignments

- Optional.
- On an AC, configure channel assignments for specified APs. Then the AC assigns the settings to the APs to instruct the AP radios to operate in specified channels.

Command	**channel** *channel-id* **radio** *radio-id*
Parameter Description	*channel-id*: specifies the operating channels of AP radios. *radio-id*: specifies the IDs of the radios assigned with channels. The value ranges from 1 to 48.
Defaults	The radio resource management (RRM) system automatically adjusts channels. By default, no channel assignments are configured.
Command Mode	AP configuration mode
Configuration	The configuration is supported only by certain APs.

Usage Guide	

Configuring the Country/Region Code Set Supported by an AC

- Optional.
- Add a country/region code to the country/region code set supported by an AC before you configure AP radios to use the country/region code.

Command	**country** *country-code*
Parameter Description	*country-code*: specifies the country/region code to be added.
Defaults	The country/region code set supported by the AC is {"CN"}.
Command Mode	AP configuration mode
Configuration Usage Guide	The country/region code "CN" supported by the AC cannot be deleted. There are two country codes available now: CN: China US: United States

Configuring a Country/Region Code

- Optional.
- Ensure that the configured country/region code is in the country/region code set supported by an AC. The AC will assign the settings to the APs to instruct the APs to use the configured country/region code.

Command	**country** *country-code* **radio** {*radio-id* | [*802.11b* | *802.11a*]}
Parameter Description	*country-code*: specifies the country/region code to be added. *radio-id*: specifies the IDs of the radios assigned with the country/region code. The value ranges from 1 to 48. *802.11b*: indicates that the country/region code is assigned to all the radios in 2.4 GHz. *802.11a*: indicates that the country/region code is assigned to all the radios in 5.8 GHz.
Defaults	The country/region code used by APs is "CN".
Command Mode	AP configuration mode
Configuration Usage Guide	1. The country/region code "CN" supported by the AC cannot be deleted. 2. The configuration is supported only by certain APs. 3. Before you configure APs, determine the country/region code set supported by the AC. If the country/region code used by an AP is changed, the RF band, channel, and power for the AP are also changed. 4. There are two country codes available now: CN (China) and US (United States). The country code is divided into indoor (IN) and outdoor (OUT), Tag the country code with I or O to identify the environment. For example, CNI indicates China Indoor. 5. If you select **802.11b**, the country/region code is configured for all the radios in 2.4 GHz. The settings take effect when the APs go online for the first time and are automatically applied to the radios. If you select **802.11a**, the condition is the same for the radios in 5.8 GHz.

Enabling Radios

- Optional.
- Enable radios on an AC. Then the AC assigns the settings to the APs to instruct the APs to enable the corresponding radios.

Command	**enable-radio** { *radio-id* | **all** }
Parameter Description	*radio-id*: specifies the IDs of the radios to be enabled. The value ranges from 1 to 48. **all**: indicates that all radios are enabled.
Defaults	By default, radios are enabled.
Command Mode	AP configuration mode
Configuration Usage Guide	When radios are enabled or disabled, the wireless STAs connected to the radios will go offline. The configuration is supported only by certain APs.

Configuring the Fragmentation Threshold

- Optional.
- On an AC, configure the fragmentation threshold for specified APs. Then the AC assigns the settings to the APs to instruct the AP radios to perform fragment logic processing according to the configured threshold.

Command	**fragment-threshold** *value* **radio** *radio-id*
Parameter Description	*value*: specifies the fragmentation threshold, which must be an even number ranging from 256 to 2346. *radio-id*: specifies the IDs of the radios assigned with the fragmentation threshold. The value ranges from 1 to 48.
Defaults	The default fragmentation threshold is 2346 bytes.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration is supported only by certain APs.

Enabling the Protection Mode

- Optional.
- On an AC, enable the protection mode for specified APs. Then the AC assigns the settings to the APs to instruct the AP radios to enable the protection mode.

Command	**green-field enable radio** *radio-id*
Parameter Description	*radio-id*: specifies the IDs of the radios enabled with the protection mode. The value ranges from 1 to 48.
Defaults	By default, the protection mode is disabled.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration takes effect only when the AP radios operate in 2.4 GHz.

Configuring the Transmit Power

- Optional.
- On an AC, configure the transmit power for specified APs. Then the AC assigns the settings to the APs to instruct the AP radios to use the transmit power.

Command	**power local** *power* **radio** {*radio-id* | [*802.11b* | *802.11a*]}
Parameter Description	*power*: specifies the percent of transmit power for APs. The value ranges from 1 to 100. *radio-id*: specifies the IDs of the radios assigned with the transmit power. The value ranges from 1 to 48. *802.11b*: indicates that the transmit power is assigned to all the radios in 2.4 GHz. *802.11a*: indicates that the transmit power is assigned to all the radios in 5.8 GHz.
Defaults	The RRM system automatically adjusts the transmit power. By default, no transmit power is configured.
Command Mode	AP configuration mode or AP group configuration mode
Configuration Usage Guide	If you select **802.11b**, the transmit power is configured for all the radios in 2.4 GHz. The settings take effect when the APs go online for the first time and are automatically applied to the radios. If you select **802.11a**, the condition is the same for the radios in 5.8 GHz. The configuration is supported only by certain APs.

Configuring a Frequency Band

- Optional.
- After a frequency band is assigned to AP radios, the RRM module analyzes the operating channel of the AP radios in global mode, adjusts the channel, and assigns the optimal channel to the AP. The AP radios are instructed to operate in the specified channel.

Command	**radio-type** *radio-id* { **802.11a** | **802.11b** }
Parameter Description	*radio-id*: specifies the IDs of the radios assigned with the frequency band. The value ranges from 1 to 48. **802.11a**: specifies the 5 GHz operating band. **802.11b**: specifies the 2.4 GHz operating band.
Defaults	A single-band AP (radio 1) supports the 2.4 GHz frequency band. For a dual-band AP, radio 1 supports the 2.4 GHz frequency band, and radio 2 supports the 5 GHz frequency band.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration is supported only by certain APs.

Configuring the RTS Threshold

- Optional.
- On an AC, configure the RTS threshold for specified APs. Then the AC assigns the settings to the APs to instruct the AP radios to use the configured threshold.

Command	**rts-threshold** *value* **radio** *radio-id*
Parameter Description	*value*: specifies the value of the RTS threshold. The value ranges from 257 to 2347, in the unit of bytes. *radio-id*: specifies the IDs of the radios assigned with the RTS threshold. The value ranges from 1 to 48.
Defaults	The default RTS threshold is 2347.
Command Mode	AP configuration mode
Configuration Usage Guide	N/A

Enabling Short GI

- Optional.
- On an AC, enable short GI for specified APs. Then the AC assigns the settings to the APs to instruct the AP radios to use short GI.

Command	**short-gi enable radio** *radio-id* **chan-width** { **20** | **40** | **80** |**160** }
Parameter Description	*radio-id*: specifies the IDs of the radios enabled with short GI. The value ranges from 1 to 48. **20**: specifies the 20 MHz bandwidth. **40**: specifies the 40 MHz bandwidth. **80**: specifies the 80 MHz bandwidth. **160**: specifies the 160 MHz bandwidth.
Defaults	By default, 40Mbps is enabled and 20Mbps is disabled.
Command Mode	AP configuration mode
Configuration Usage Guide	N/A

Configuring the Preamble Type

- Optional.
- On an AC, configure the preamble type for specified APs. Then the AC assigns the settings to the APs to instruct the AP radios to use the configured preamble type.

Command	**preamble** { **long** | **short** } **radio** *radio-id*
Parameter Description	**long**: indicates that APs transmit only the frames with long preambles. **short**: indicates that APs can transmit the frames with short or long preambles. *radio-id*: specifies the IDs of the radios assigned with the preamble type. The value ranges from 1 to 48.
Defaults	By default, the short preamble type is supported.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration is supported only by certain APs.

Configuring the Short Slot Time

- Optional.
- On an AC, configure the short slot time for specified APs. Then the AC assigns the settings to the APs to instruct the AP radios to enable the short slot time feature.

Command	**short-slot-time radio** *radio-id*
Parameter Description	*radio-id*: specifies the IDs of the radios assigned with the short slot time. The value ranges from 1 to 48.
Defaults	By default, the short slot time function is enabled.
Command Mode	AP configuration mode
Configuration Usage Guide	N/A

Enabling TSC Update

- Optional.
- On an AC, enable TSC update for specified APs. Then the AC assigns the settings to the APs to instruct the AP to enable TSC update.

Command	**update-key-tsc enable**
Parameter Description	N/A
Defaults	By default, TSC update is disabled.
Command Mode	AP configuration mode or AP group configuration mode
Configuration Usage Guide	N/A

Configuring the Maximum Distance of Wireless Transmission Between APs and the Peer End

- Optional.
- On an AC, configure the maximum distance of wireless transmission between APs and the peer end for specified APs. Then the AC assigns the settings to the APs to instruct the AP radios to send and receive packets according to the maximum distance.

Command	**peer-distance** *val* **radio** *radio-id*
Parameter Description	*val*: specifies the maximum wireless transmission distance allowed by APs. The value ranges from 1000 to 25000, in the unit of m. *radio-id*: specifies the IDs of the radios assigned with the maximum wireless transmission distance. The value ranges from 1 to 48.
Defaults	By default, the maximum wireless transmission distance is 1000 m.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration is supported only by certain APs.Perform the configuration only when the actual maximum distance of wireless transmission between APs and the peer end is greater than 1000 m. You can set the distance to a large value but do not set it to a value smaller than the actual distance.

Configure MIMO for Multi Users

- Optional.
- After this command is configured, the AC will deliver the configuration to the AP to enable the MU-MIMO function on the AP.

Command	**mu-mimo enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the radio ID, in the range from 1 to 48.
Defaults	If the radio does not support the mu-mimo function, the AC does not support it by default. If the radio supports the mu-mimo function and it is enabled on the AP by default, it is enabled on the AC by default. If the radio supports the mu-mimo function and it is disabled on the AP by default, it is disabled on the AC by default.
Command Mode	AP configuration mode all-AP configuration mode

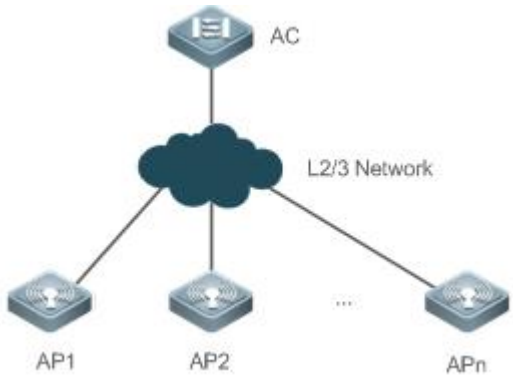
	AP group configuration mode
Configuration Usage Guide	N/A

Verification

- Run **show ap-config running** *ap-name* to display the parameter settings of STA access control.

Configuration Example

Configuring AP RF Parameters

Scenario Figure 4-5	 In Figure 4-5 an AC is connected to fit APs. On the AC, configure the RF parameters for AP1 according to the following steps: 1. Set the global country code to CN. 2. Configure support for CN on the AC. 3. Enable A-MPDU for radio 1 of AP1. 4. Set the maximum 802.11n MCS index value to 15 for radio 1 of AP1. 5. Set the maximum 802.11ac MCS index value to 19 for radio 1 of AP1. 6. Set the antenna selection masks of the transmit type and receive type to 7 and 5 respectively for radio 1 of AP1. 7. Enable usage of external antennas and disable usage of internal antennas for radio 1 of AP1. 8. Set the beacon frame transmission period to 200 ms for radio 1 of AP1. 9. Configure the "CN" country code for radio 1 of AP1. 10. Assign channel 11 to radio 1 of AP1. 11. Assign the 20 MHz bandwidth to radio 1 of AP1. 12. Enable short GI for radio 1 of AP1 in 20 MHz. 13. Enable the protection mode for radio 1 of AP1. 14. Configure the short preamble type for radio 1 of AP1. 15. Configure the short slot time for radio 1 of AP1. 16. Configure the country code “CN” for radio 2 of AP1. 17. Assign channel 149 to radio 2 of AP1. 18. Assign the 40 MHz bandwidth to radio 2 of AP1. 19. Enable radio 2 of AP1. 20. Set the fragmentation threshold to 2346 bytes for radio 2 of AP1. 21. Set the percent of transmit power to 100% for radio 2 of AP1. 22. Set the RTS threshold to 2347 bytes for radio 2 of AP1. 23. Enables TSC update for AP1. 24. Set the maximum distance of wireless transmission between APs and the peer end to 3000 m for radio 1 of AP1. 25. Enable MU-MIMO on AP1 Radio 2.
	26. Set the maximum distance of wireless transmission between APs and the peer end to 3000mradio 1 of AP1. 27. Enable MU-MIMO for radio 2 of AP1. 28. Enable ofdma for radio 2 of AP1.

Configuration Steps	● On the AC, configure the RF parameters for AP1.
	FS# configure terminal FS(config)# Rac-controller FS(config-ac)# country CN FS(config-ac)#R exit FS(config)# ap-config AP1 FS(config-ap)# 802.11n a-mpdu enable radio 1 FS(config-ap)# 802.11n mcs support 15 radio 1 FS(config-ap)# 802.11ac mcs support 19 radio 1 FS(config-ap)# antenna transmit 7 radio 1 FS(config-ap)# antenna receive 5 radio 1 FS(config-ap)# external-antenna enable radio 1 FS(config-ap)# beacon period 200 radio 1 FS(config-ap)# country CN radio 1 FS(config-ap)# channel 11 radio 1 FS(config-ap)# chan-width 20 radio 1 FS(config-ap)# short-gi enable radio 1 chan-width 20 FS(config-ap)# green-field enable radio 1 FS(config-ap)# preamble short radio 1 FS(config-ap)# short-slot-time radio 1 FS(config-ap)# country CN radio 2 FS(config-ap)# channel 149 radio 2 FS(config-ap)# chan-width 40 radio 2 FS(config-ap)# enable-radio 2 FS(config-ap)# fragment-threshold 2346 radio 2 FS(config-ap)# power local 100 radio 2 FS(config-ap)# rts-threshold 2347 radio 2 FS(config-ap)# update-key-tsc enable FS(config-ap)# peer-distance 3000 radio 1 FS(config-ap)# mu-mimo enable radio 2
Verification	● Run **show ap-config running** *ap-name* to display the RF parameter settings of AP1.
	FS(config)# show ap-config running AP1 ! ap-config AP1 802.11n mcs support 15 radio 1 802.11n mcs support 15 radio 2 802.11ac mcs support 19 radio 1 update-key-tsc enable

```
 short-gi enable radio 1 chan-width 20
 green-field enable radio 1
 station-role root-ap radio 1
 station-role root-ap radio 2
 chan-width 40 radio 2
 antenna receive 5 radio 1
external-antenna enable radio 1
 channel 11 radio 1
 channel 149 radio 2
 beacon period 200 radio 1
 power local 100 radio 2
peer-distance 3000 radio 1
!
```

4.4.4 Configuring Data Rate Control Parameters

Configuration Effect

- Configure the data rate control parameters for fit APs centrally for easier configuration management.

Configuration Steps

Configuring the Data Rate Set Supported by 802.11a STAs

- Optional.
- On an AC, configure the data rate set supported by 802.11a STAs. Then the AC assigns the settings to all the APs to instruct the APs to apply the configured data rate set to 802.11a STAs.

Command	**802.11a network rate** { **6** | **9** | **12** | **18** | **24** | **36** | **48** | **54** } { **disabled** | **mandatory** | **supported** }
Parameter Description	**6**: specifies the 6 Mbps data rate. **9**: specifies the 9 Mbps data rate. **12**: specifies the 12 Mbps data rate. **18**: specifies the 18 Mbps data rate. **24**: specifies the 24 Mbps data rate. **36**: specifies the 36 Mbps data rate. **48**: specifies the 48 Mbps data rate. **54**: specifies the 54 Mbps data rate. **disabled**: indicates that the data rate set is not supported. **mandatory**: indicates that support for the data rate set is mandatory. **supported**: indicates that support for the data rate set is optional.
Defaults	Support for the 6 Mbps, 12 Mbps, and 24 Mbps data rates is mandatory, whereas support for the 9 Mbps, 18 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps data rates is optional.
Command	AC configuration mode/AP configuration mode/AP group configuration mode

Mode	
Configuration Usage Guide	N/A

Configuring the Data Rate Set Supported by 802.11b STAs

- Optional.
- On an AC, configure the data rate set supported by 802.11b STAs. Then the AC assigns the settings to all the APs to instruct the APs to apply the configured data rate set to 802.11b STAs.

Command	**802.11b network rate** { **1** | **2** | **5** | **11** } { **disabled** | **mandatory** | **supported**}
Parameter Description	**1**: specifies the 1 Mbps data rate. **2**: specifies the 2 Mbps data rate. **5**: specifies the 5.5 Mbps data rate. **11**: specifies the 11 Mbps data rate. **disabled**: indicates that the data rate set is not supported. **mandatory**: indicates that support for the data rate set is mandatory. **supported**: indicates that support for the data rate set is optional.
Defaults	Support for the 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps data rates is mandatory.
Command Mode	AC configuration mode/AP configuration mode/AP group configuration mode
Configuration Usage Guide	N/A

Configuring the Data Rate Set Supported by 802.11g STAs

- Optional.
- On an AC, configure the data rate set supported by 802.11g STAs. Then the AC assigns the settings to all the APs to instruct the APs to apply the configured data rate set to 802.11g STAs.

Command	**802.11g network rate** { **1** | **2** | **5** | **6** | **9** | **11** | **12** | **18** | **24** | **36** | **48** | **54** } { **disabled** | **mandatory** | **supported**}
Parameter Description	**1**: specifies the 1 Mbps data rate. **2**: specifies the 2 Mbps data rate. **5**: specifies the 5.5 Mbps data rate. **6**: specifies the 6 Mbps data rate. **9**: specifies the 9 Mbps data rate. **11**: specifies the 11 Mbps data rate. **12**: specifies the 12 Mbps data rate. **18**: specifies the 18 Mbps data rate. **24**: specifies the 24 Mbps data rate. **36**: specifies the 36 Mbps data rate. **48**: specifies the 48 Mbps data rate. **54**: specifies the 54 Mbps data rate. **disabled**: indicates that the data rate set is not supported. **mandatory**: indicates that support for the data rate set is mandatory. **supported**: indicates that support for the data rate set is optional.

Defaults	Support for the 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps data rates is mandatory, whereas support for the 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps data rates is optional.
Command Mode	AC configuration mode/AP configuration mode/AP group configuration mode
Configuration Usage Guide	N/A

Configuring the Multicast Rate

- Optional.
- On an AC, configure the multicast rate for a WLAN. Then the AC assigns the settings to all the APs on the WLAN to instruct the APs to apply the configured multicast rate within the range of the WLAN.

Command	**mcast-rate** *mcas-num*
Parameter Description	*mcast-num*: specifies the WLAN multicast rate. The 1 Mbps, 6 Mbps, 11 Mbps, 24 Mbps, and 54 Mbps options are available.
Defaults	The default multicast rate is 24 Mbps.
Command Mode	WLAN configuration mode
Configuration Usage Guide	N/A

Configuring the Beacon Frame Transmission Rate

- Optional.
- On an AC, configure the beacon frame transmission rate for specified APs. Then the AC assigns the settings to the APs to instruct the APs to transmit beacon frames according to the configured rate.

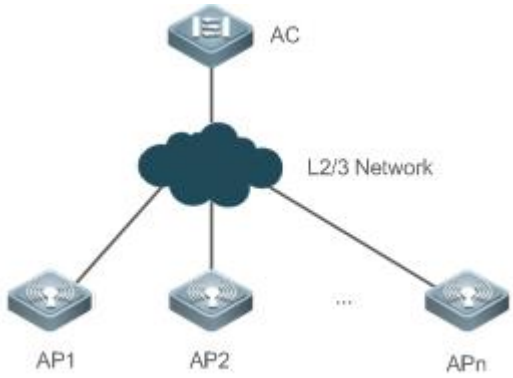
Command	**beacon rate** *rate-Mbps* **radio** {*radio-id* | [*802.11b* | *802.11a*]}
Parameter Description	*rate_Mbps*: specifies the rate at which beacon frames are transmitted. *radio-id*: specifies the IDs of the radios assigned with the beacon frame transmission rate. The value ranges from 1 to 48. *802.11b*: indicates that the beacon frame transmission rate is assigned to all the radios in 2.4 GHz. *802.11a*: indicates that the beacon frame transmission rate is assigned to all the radios in 5.8 GHz.
Defaults	By default, no beacon frame transmission rate is configured.
Command Mode	AP configuration mode
Configuration Usage Guide	1. Do not configure a beacon frame transmission rate that is disabled in the data rate set settings. 2. Because the 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps rates are not supported in 5 GHz, do not set the beacon frame transmission rate to any of the preceding values for the radios in 5 GHz. 3. If you select **802.11b**, the beacon frame transmission rate is configured for all the radios in 2.4 GHz. The settings take effect when the APs go online for the first time and are automatically applied to the radios. If you select **802.11a**, the condition is the same for the radios in 5.8 GHz.

Verification

- Run **show running** to display the parameter settings of data rate control.

Configuration Example

Configuring Data Rate Control Parameters

Scenario **Figure 4-6**	 In Figure 4-6, an AC is connected to fit APs. On the AC, configure the data rate control parameters according to the following steps: 1. Disable the 6 Mbps rate for 802.11a STAs. 2. Disable the 1 Mbps, 2 Mbps, and 5.5 Mbps rates for 802.11b STAs. 3. Disable the 1 Mbps, 2 Mbps, and 5.5 Mbps rates for 802.11g STAs. 4. Set the multicast rate for WLAN1 to 54 Mbps.
	On the AC, configure the data rate control parameters for AP1 according to the following step: 1. Configure the beacon frame transmission rate for radio 1 of AP1.
Configuration Steps	● On the AC, configure the data rate control parameters.
	FS# configure terminal FS(config)# ac-controller FS(config-ac)# 802.11a network rate 6 disabled FS(config-ac)# 802.11b network rate 1 disabled FS(config-ac)# 802.11b network rate 2 disabled FS(config-ac)# 802.11b network rate 5 disabled FS(config-ac)# 802.11g network rate 1 disabled FS(config-ac)# 802.11g network rate 2 disabled FS(config-ac)# 802.11g network rate 5 disabled FS(config-ac)# exit FS(config)# wlan-config 1 FS(config-wlan)# mcast-rate 54
	● On the AC, configure the beacon frame transmission rate for AP1.

	FS# configure terminal FS(config)# ap-config AP1 FS(config-ap)# beacon rate 12.0 radio 1
Verification	● Run **show running-config** to display the parameter settings of data rate control.

	FS# show running-config
	...
	!
	wlan-config 1 ss
	  enable-broad-ssid
	  mcast-rate 54
	!
	...
	!
	ac-controller
	  country CN
	  802.11g network rate 1 disabled
	  802.11g network rate 2 disabled
	  802.11g network rate 5 disabled
	  802.11g network rate 11 mandatory
	  802.11g network rate 6 supported
	  802.11g network rate 9 supported
	  802.11g network rate 12 supported
	  802.11g network rate 18 supported
	  802.11g network rate 24 supported
	  802.11g network rate 36 supported
	  802.11g network rate 48 supported
	  802.11g network rate 54 supported
	  802.11b network rate 1 disabled
	  802.11b network rate 2 disabled
	  802.11b network rate 5 disabled
	  802.11b network rate 11 mandatory
	  802.11a network rate 6 disabled

	802.11a network rate 9 supported 802.11a network rate 12 mandatory 802.11a network rate 18 supported 802.11a network rate 24 mandatory 802.11a network rate 36 supported 802.11a network rate 48 supported 802.11a network rate 54 supported ! ...
	● Run **show ap-config running** *ap-name* to display the beacon frame transmission rate settings of AP1.
	FS(config)# show ap-config running AP1 ! ap-config AP1 channel 11 radio 1 channel 149 radio 2 beacon period 200 radio 1 beacon rate 12.0 radio 1 power local 100 radio 2 !

4.4.5 Configuring Power-Save Parameters

Configuration Effect

- Configure the power-save parameters for fit APs centrally for easier configuration management.

Configuration Steps

Configuring the DTIM Period

- Optional.
- The power saving effect is improved if the DTIM period is set to a large value, but the delay for downstream multicast packets is increased.

Command	**beacon dtim-period** *period-num* **radio** *radio-id*
Parameter Description	*period-num*: specifies the DTIM period. The value ranges from 1 to 255. The unit is expressed as the period of one beacon frame. *radio-id*: specifies the IDs of the radios assigned with the DTIM period. The value ranges from 1 to 48.
Defaults	The unit of the DTIM period is expressed as the period of one beacon frame.
Command Mode	AP configuration mode

Configuration Usage Guide	N/A

Enabling or Disabling U-APSD Power Saving

- Optional.
- Enable U-APSD power saving to reduce the delay of the services with high real-time requirements during the power management process. The transmission of radio signals can be disabled during most of the time to extends the battery life.

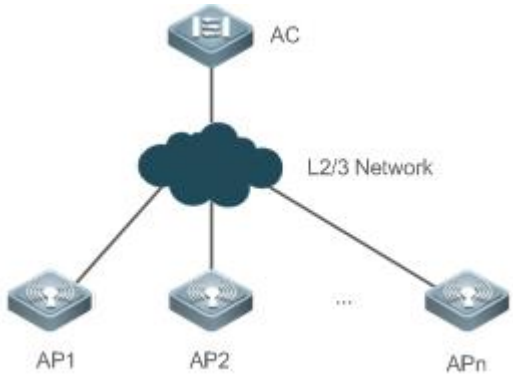
Command	**apsd** { **enable** | **disable** } **radio** *radio-id*
Parameter Description	**enable**: enables U-APSD power saving. **disable**: disables U-APSD power saving. *radio-id*: specifies the IDs of the radios enabled with U-APSD power saving. The value ranges from 1 to 48.
Defaults	By default, U-APSD power saving is enabled.
Command Mode	AP configuration mode
Configuration Usage Guide	N/A

Verification

- Run **show ap-config running** *ap-name* to display the power-save parameter settings.

Configuration Example

Configuring Power-Save Parameters

Scenario Figure 4-7	
Configuration Steps	• On the AC, set the DTIM period to 3 for radio 1 of AP1. • On the AC, enable U-APSD power saving for radio 1 of AP1.
	FS#configure terminal FS(config)#ap-config AP0001 FS(config-ap)#beacon dtim-period 3 radio 1 FS(config-ap)#apsd enable radio 1

Verification	● Run **show ap-config running** *ap-name* to display the power-save parameter settings of AP1.
	FS(config)# show ap-config running AP1 ! ap-config AP1 802.11n mcs support 15 radio 1 802.11n mcs support 15 radio 2 update-key-tsc enable short-gi enable radio 1 chan-width 20 green-field enable radio 1 station-role root-ap radio 1 station-role root-ap radio 2 chan-width 40 radio 2 antenna receive 5 radio 1 channel 11 radio 1 channel 149 radio 2 beacon period 200 radio 1 beacon dtim-period 3 radio 1 power local 100 radio 2 !

4.4.6 Enabling Link Integrity Detection

Configuration Effect

- Enable link integrity detection.

Configuration Steps

Enabling Link Integrity Detection

- (Mandatory) Run **link-check enable** to enable link integrity detection.

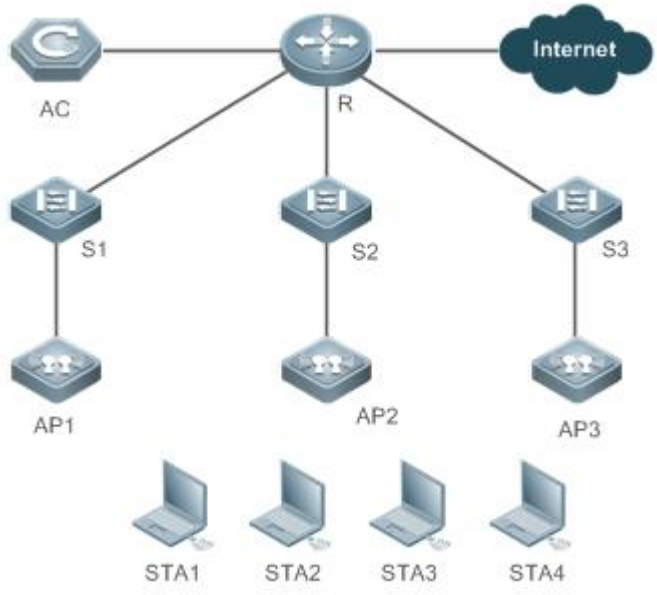
Command	**link-check enable**
Parameter Description	N/A
Defaults	By default, link integrity detection is disabled.
Command Mode	Global configuration mode
Configuration Usage Guide	By default, link integrity detection is disabled.

Verification

- Run **show running-config** to display the configuration status of link integrity detection.

Configuration Example

Enabling Link Integrity Detection

Scenario **Figure 4-8**	 In Figure 4-8, an AC is connected to fit APs. Enable link integrity detection according to the following step: 1. Enable link integrity detection.
Configuration Steps	● Enable link integrity detection on the AC.
	FS# configure terminal FS(config)# link-check enable
Verification	● Run **show running-config** to display the configuration status of link integrity detection.
	FS(config)# show running-config …… link-check enable ……

4.4.7 Configuring E-Bag Parameters

Configuration Effect

- Configure the E-bag parameters for APs and radios for easier configuration management.

Configuration Steps

Configuring the A-MPDU Software Retransmission Times

- Optional.
- On an AC, configure the A-MPDU software retransmission times for specified APs. Then the AC assigns the settings to the APs to instruct the APs to transmit A-MPDU packets according to the configured times.
- The greater the retransmission times, the lower the probability of sub-frame loss. If packets are retransmitted frequently, the burden on the air interface is increased, which affects the real-time transmission of packets on the air interface. You can increase the retransmission times if you need to avoid packet loss when there is a high probability of sub-frame loss.

Command	**ampdu-retries** *times* **radio** *radio-id*
Parameter Description	*times*: specifies the A-MPDU software retransmission times. The value ranges from 1 to 10. *radio-id*: specifies the IDs of the radios assigned with the A-MPDU software retransmission times. The value ranges from 1 to 48.
Defaults	By default, the A-MPDU software retransmission times is 10.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration takes effect only when the AP radios operate in 802.11n or 802.11ac mode. The configuration is supported only by certain APs.

Enabling or Disabling RTS Protection for A-MPDU Packets

- Optional.
- On an AC, enable RTS protection for A-MPDU packets for specified APs. Then the AC assigns the settings to the APs to instruct the APs to transmit A-MPDU packets using RTS protection.
- Enable RTS protection only when the resource waste on the air interface caused by hidden nodes is greater than the resource consumption of RTS interaction on the air interface.

Command	**ampdu-rts radio** {*radio-id* | [*802.11b* / *802.11a*]}
Parameter Description	*radio-id*: specifies the IDs of the radios enabled with RTS protection. The value ranges from 1 to 48. *802.11b*: indicates that RTS protection is enabled for all the radios in 2.4 GHz. *802.11a*: indicates that RTS protection is enabled for all the radios in 5.8 GHz.
Defaults	By default, RTS protection for A-PMDU packets is disabled.
Command Mode	AP configuration mode
Configuration Usage Guide	If you select **802.11b**, RTS protection for A-PMDU packets is enabled for all the radios in 2.4 GHz. The settings take effect when the APs go online for the first time and are automatically applied to the radios. If you select **802.11a**, the condition is the same for the radios in 5.8 GHz. The configuration takes effect only when the AP radios operate in 802.11n or 802.11ac mode.

Configuring the Single-Time Received Ethernet Packet Quantity for APs

- Optional.
- By default, the single-time received Ethernet packet quantity varies with different APs.

- On an AC, configure the single-time received Ethernet packet quantity for specified APs. Then the AC assigns the settings to the APs to instruct the APs to limit the number of Ethernet packets received at a single time according to the settings. Increasing Ethernet packet reception can improve network performance but may reduce APs' ability to handle key packets in real time. You can reduce Ethernet packet reception when the requirements for performance are not high but user concurrency and real-time packet handling are demanded. In this case, it is recommended that the single-time received Ethernet packet quantity be set to 25.

Command	**eth-schd** *limit*
Parameter Description	*limit*: specifies the number of Ethernet packets received at a single time. The value ranges from 1 to 256.
Defaults	By default, the single-time received Ethernet packet quantity varies with different APs.
Command Mode	AP configuration mode
Configuration Usage Guide	N/A

Enabling or Disabling LDPC

- Optional.
- On an AC, enable LDPC for specified APs. Then the AC assigns the settings to the APs to instruct the APs to send and receive packets using LDPC.
- LDPC improves the coding reliability and gains. It also greatly reduces the probability of information loss during transmission in frequencies with serious noise interference. However, a small number of STAs are not compatible with LDPC, and enabling LDPC will result in packet loss.

Command	**ldpc radio** *radio-id*
Parameter Description	*radio-id*: specifies the IDs of the radios enabled with LDPC. The value ranges from 1 to 48.
Defaults	By default, LDPC is enabled.
Command Mode	AP configuration mode
Configuration Usage Guide	N/A

Enabling or Disabling Transmit/Receive STBC

- Optional.
- On an AC, enable transmit/receive STBC for specified APs. Then the AC assigns the settings to the APs to instruct the APs to send and receive packets using STBC.
- STBC improves the reliability of data transmission. Some STAs may not be compatible with STBC.

Command	**stbc radio** *radio-id*
Parameter Description	*radio-id*: specifies the IDs of the radios enabled with STBC. The value ranges from 1 to 48.
Defaults	By default, STBC is enabled.
Command Mode	AP configuration mode

Configuration Usage Guide	N/A

Configuring E-bag Network Optimization in One-Click Mode

- Optional.
- Run **ebag** in AP configuration mode to quickly configure E-bag network optimization in one-click mode.
- The AP320, AP330, and AP3220 are optimized in the following aspects:

- Packet handling optimization on wired ports: **eth-schd 25**
- Optimization of wireless aggregate packet retransmission: **ampdu-retries 2**
- WiFox is disabled.

- The AP530 is optimized in the following aspects:

- By default, radios 1 and 2 use the sta-idle-time 1800 settings.
- Radio 1 optimization: The 1 Mbps, 2 Mbps, and 5.5 Mbps mandatory rates are disabled for 802.11b/g STAs, and the 11 Mbps and 24 Mbps rates are configured as mandatory rates for 802.11g STAs. RTS protection for A-MPDU packets is enabled.

- On an AC, configure E-bag network optimization for specified APs. Then the AC assigns the settings to the APs to instruct the APs to send and receive packets according to the settings.

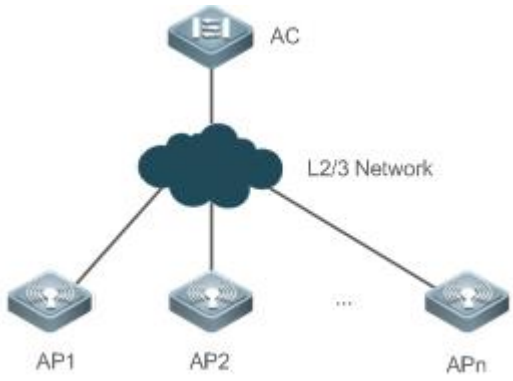
Command	**ebag**
Parameter Description	N/A
Defaults	No default settings are available.
Command Mode	AP configuration mode
Configuration Usage Guide	Use this command only when E-bag is configured. If E-bag is not configured, do not use this command unless necessary.

Verification

- Run **show ap-config running** *ap-name* to display the E-bag parameter settings.

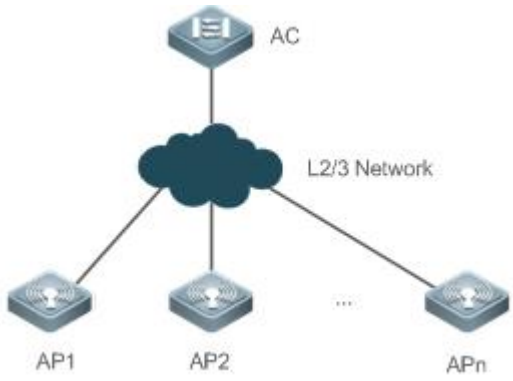
Configuration Example

Configuring E-Bag Parameters

Scenario **Figure 4-9**	

	In Figure 4-9, an AC is connected to APs. On the AC, configure the E-bag parameters for AP1 according to the following steps: 1. Set the A-MPDU software retransmission times to 3 for radio 1 of AP1. 2. Enable RTS protection for A-MPDU packets for radio 1 of AP1. 3. Set the single-time received Ethernet packet quantity to 100 for AP1. 4. Disable LDPC for radio 1 of AP1. 5. Disable transmit/receive STBC for radio 1 of AP1.
Configuration Steps	● On the AC, configure the RF parameters for AP1.
	FS# configure terminal FS(config)# ap-config AP1 FS(config-ap)# ampdu-retries 3 radio 1 FS(config-ap)# ampdu-rts radio 1 FS(config-ap)# eth-schd 100 FS(config-ap)# no ldpc radio 1 FS(config-ap)# no stbc radio 1
Verification	● Run **show ap-config running** *ap-name* to display the E-bag parameter settings of AP1.
	FS(config)# show ap-config running AP1 ! ap-config AP1 ap-mac 00d0.f801.0528 country US radio 1 channel 11 radio 1 no 11acsupport enable radio 2 ampdu-retries 3 radio 1 ampdu-rts radio 1 no stbc radio 1 no ldpc radio 1 eth-schd 100 wmm edca-radio video aifsn 1 cwmin 3 cwmax 4 txop 90 radio 1 wmm edca-radio back-ground aifsn 7 cwmin 4 cwmax 10 txop 5 radio 2 !

Configuring E-bag Network Optimization in One-Click Mode

Scenario **Figure 4-10**	 In Figure 4-10, an AC is connected to fit APs. AP1 is configured with E-bag settings. On the AC, configure E-bag network optimization for AP1 in one-click mode.
Configuration Steps	● On the AC, configure E-bag network optimization for AP1 in one-click mode.
	FS# configure terminal FS(config)# ap-config AP1 FS(config-ap)# ebag
Verification	● Run **show ap-config running** *ap-name* to display the E-bag parameter settings of AP1.
	FS(config)# show ap-config running AP1 ! ap-config AP1 ap-mac 00d0.f801.0528 country US radio 1 channel 11 radio 1 no 11acsupport enable radio 2 ampdu-retries 2 radio 1 ampdu-retries 2 radio 2 eth-schd 25 ebag wmm edca-radio video aifsn 1 cwmin 3 cwmax 4 txop 90 radio 1 wmm edca-radio back-ground aifsn 7 cwmin 4 cwmax 10 txop 5 radio 2 !

4.4.8 Configuring WLANs in One-Click Mode

Configuration Effect

- Configure WLANs quickly on devices with zero configurations in one-click mode. The one-click WLAN configuration feature helps the land survey personnel improve operation efficiency and the channel personnel execute performance tests conveniently.

Configuration Steps

Configuring WLANs in One-Click Mode

- Optional.
- Run **autowifi** in configuration mode to configure WLANs in one-click mode, thus realizing fast configuration of wireless networks. The one-click WLAN configuration feature helps the land survey personnel improve operation efficiency and the channel personnel execute performance tests conveniently.

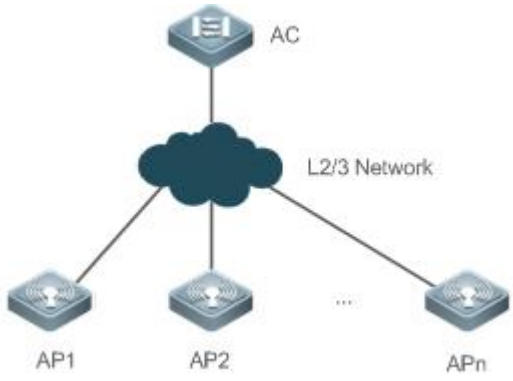
Command	**autowifi**
Parameter Description	N/A
Defaults	No default settings are available.
Command Mode	AC global configuration mode
Configuration Usage Guide	The one-click WLAN configuration feature allows you to perform fast configuration on devices with zero configurations. The one-click WLAN configuration feature helps the land survey personnel improve operation efficiency and the channel personnel execute performance tests conveniently.

Verification

- Run **show running** to display the one-click WLAN configuration.

Configuration Example

Configuring WLANs in One-Click Mode

Scenario **Figure 4-11**	 In Figure 4-11, an AC is connected to fit APs. Configure WLANs in one-click mode on the AC.
Configuration	- Configure WLANs in one-click mode on the AC.

Steps	
	FS# configure terminal FS(config)# autowifi
Verification	● Run **show running** to display the one-click WLAN configuration.

	FS(config)# show running
	!
	wlan-config 1 autowifi_1234
	!
	ap-group default
	  interface-mapping 1 2 ap-wlan-id 1
	!
	ap-config all
	  fair-schedule
	!
	ac-controller
	
	  802.11g network rate 1 mandatory
	  802.11g network rate 2 mandatory
	  802.11g network rate 5 mandatory
	  802.11g network rate 6 supported
	  802.11g network rate 9 supported
	  802.11g network rate 11 mandatory
	  802.11g network rate 12 supported
	  802.11g network rate 18 supported
	  802.11g network rate 24 supported
	  802.11g network rate 36 supported
	  802.11g network rate 48 supported
	  802.11g network rate 54 supported
	  802.11b network rate 1 mandatory
	  802.11b network rate 2 mandatory
	  802.11b network rate 5 mandatory
	  802.11b network rate 11 mandatory
	  802.11a network rate 6 mandatory

```
 802.11a network rate 9 supported
 802.11a network rate 12 mandatory
 802.11a network rate 18 supported
 802.11a network rate 24 mandatory
 802.11a network rate 36 supported
 802.11a network rate 48 supported
 802.11a network rate 54 supported
!
ip dhcp pool web_ap_pool_1
 option 138 ip 88.88.88.88
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
!
ip dhcp pool web_sta_pool_1
 network 192.168.2.0 255.255.255.0
 dns-server 8.8.8.8
 default-router 192.168.2.1
!
link-check disable
!
vlan 1
!
vlan 2
!
interface Loopback 0
 ip address 88.88.88.88 255.255.255.255
!
interface VLAN 1
 ip address 192.168.1.1 255.255.255.0
!
interface VLAN 2
 ip address 192.168.2.1 255.255.255.0
!
wlansec 1
```

	security rsn enable security rsn ciphers aes enable security rsn akm psk enable security rsn akm psk set-key ascii autowifi !

4.5 Monitoring

Displaying

Description	Command
Displays the link information of wireless STAs.	**linktest**
Displays the AP list that maps the 802.11a or 802.11b network on an AC.	**show ac-config** { **802.11a** | **802.11b** } **summary**
Displays the antenna feeder status of all APs.	**show antenna all**
Displays the antenna feeder status of an AP.	**show antenna single** *ap-name*
Displays the radio information of all APs.	**show ap-config radio**
Displays the radio information of an AP.	**show ap-config radio ap-name** *ap-name*
Displays the configuration information of an AP radio.	**show ap-config radio** *radio-id* **config** *ap-name*
Displays the status information of an AP radio.	**show ap-config radio** *radio-id* **status** *ap-name*
Displays the radio list of an AP.	**show ap-config radio status** *ap-name*
Displays the radio information of all APs.	**show ap-config summary radio**
Displays the STA information mapped to a MAC address.	**show client details** *sta-mac*

5 Configuring ETH-MNG

5.1 Overview

ETH-MNG (Ethernet Management) is used to configure AP wired paramters.

LAN bandwidth limiting is a basic service of ETH-MNG, preventing wired clients occupying too much bandwidth.

5.1.1 Protocols and Standards

- N/A

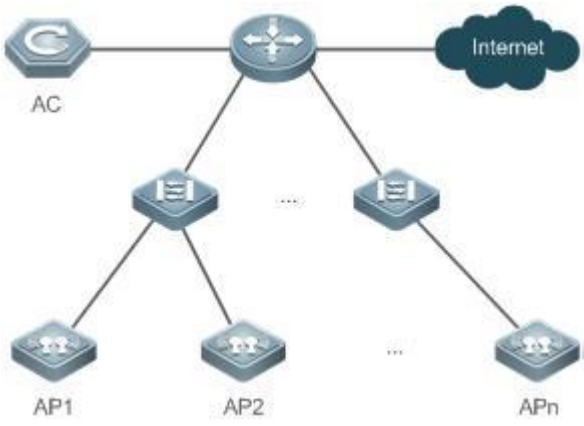
5.2 Applications

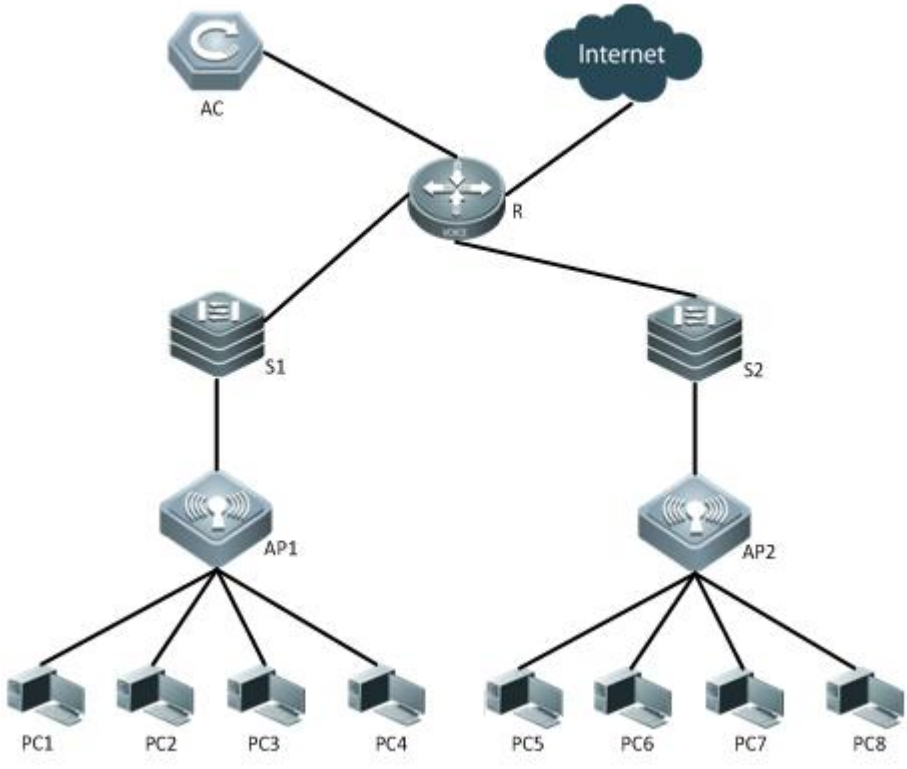
Application	Description
Configuring Fit APs	Configure fit AP parameters.
Configuring LAN Bandwidth Limit	Configure the max bandwitdth of each LAN port in a fit AP architecture.

5.2.1 Configuring Fit APs

Scenario

Provision fit APs to allow the administrator to manage APs on an AC.Figure 5-1





Deployment

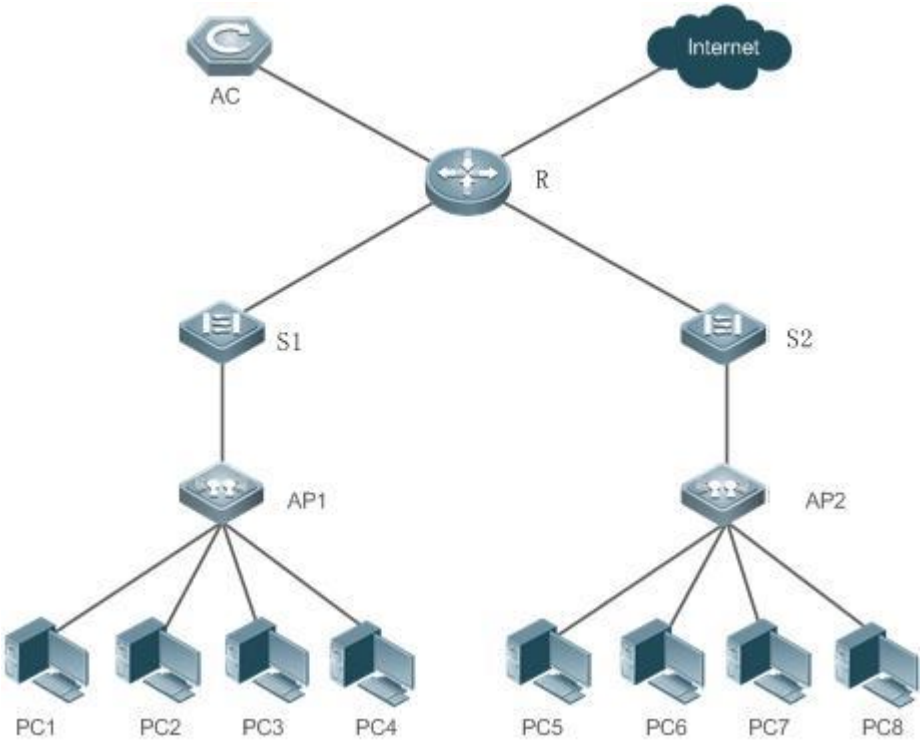
Configure a bandwitdth limit on each LAN port.

5.2.2 Configuring LAN Bandwidth Limit

Scenario

Configuring LAN bandwitdth limiting on each LAN port in a fit AP architecture.

- An AC is connected to the Internet through a router. Two APs (AP1 and AP2) are connected to the router through two switches, and are associated with the AC.
- PC1, PC2, PC3, and PC4 are associated with AP1; PC5, PC6, PC7, and PC8 are associated with AP2. These PCs access the Internet through the AC.



Notes

R is a network egress router.

S1 and S2 are Layer 2 (L2) switches, and serve as the access devices of the APs.

AP1 is directly connected to S1, and AP2 to S2.

Deployment

- The L2 switches provide the access function for the APs.
- The router R is connected to the network formed by the AC and the APs. It is also connected to the PCs and the Internet.
- Configure bandwidth limit on each LAN port.

5.3 Features

Basic Concepts

N/A

Overview

Feature	Description
LAN Bandwidth Limit	Configure the maximum bandwidth of various LAN ports of APs so as to avoid the slow Internet access of wireless users in a scenario where wireless and wired users coexist and wired users occupy a substantial bandwidth.

5.3.1 LAN Bandwidth Limiting

Working Principle

The LAN bandwidth limiting is used to configure the maximum bandwidth of various LAN ports of APs so as to avoid the slow Internet access of wireless users caused in a scenario where wireless and wired users coexist and wired users occupy a substantial bandwidth.

5.4 Configuration

Configuration	Description and Command	
Configuring LAN Bandwitdth Limit	(Optional) It is used to configure the bandwidth limit for each LAN port.	
	wired-rate *value* [**port** *port-id*]	Configures LAN bandwidth limit on the AC.
	wired-rate *value*	Configures LAN bandwidth limit on the AP.

5.4.1 LAN Bandwidth Limiting

Networking Requirements

- Configure the bandwidth limit for LAN ports.

Notes

- N/A

Configuration Steps

Configuring the LAN Bandwidth Limit

- The configuration is optional.
- Perform this configuration on the AC or on a fat AP.
- Run the **wired-rate** command to configure the LAN bandswith limit.

Command	**Fit AP**: **wired-rate** *value* [**port** *port-id*] **Fat AP**: **wired-rate** *value*
Parameter Description	If no port is specified, all ports are configured.
Defaults	By default, no bandwidth limit is configured.
Command Mode	Fit AP: AP configuration mode/AP group configuration mode Fat AP: Interface configuraton mode
Usage Guide	N/A

Verification

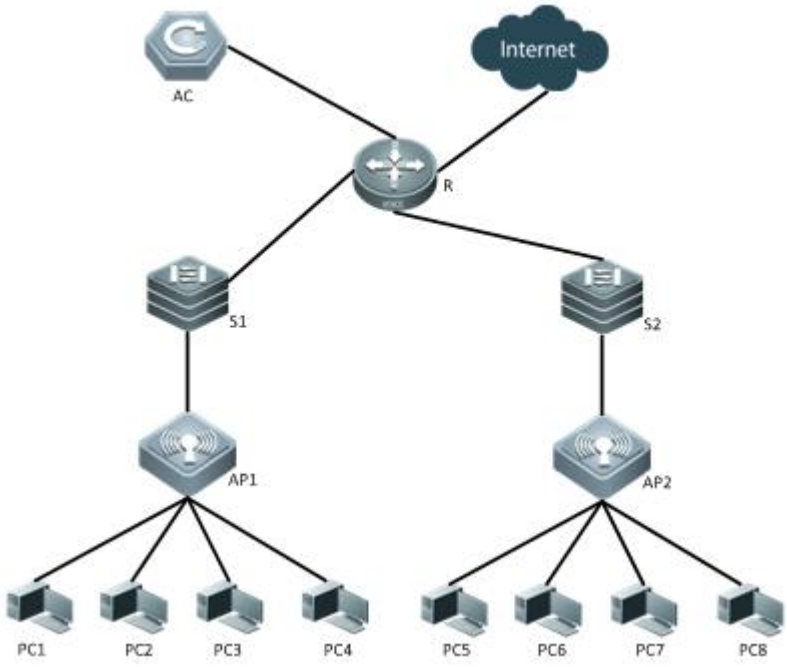
- Run the **show running-config** command to display the configuration about the bandwidth limit of various LAN ports.

Configuration Example

Configuring LAN Bandwidth Limiting

Scenario

Figure 5-2



Configure LAN bandwidth limit in the fit AP environment, as shown in Figure 5-2.

1. Configure the LAN bandwidth limit

Configuration Steps	● On the AC, set the maximum bandwidth of port 3 on the AP to 30 Mbps.
AC	FS(config)# ap-config [ap-name] FS(config-ap)# wired-rate 30 port 3 ● On the AC, set the maximum bandwidth of port 3 on the group APs to 30 Mbps. FS(config)# ap-group default FS(config-group)#wired-rate 30 port 3 ● On the AC, set the maximum bandwidth of all LAN ports on the group APs to 30 Mbps. FS(config)# ap-group default FS(config-group)#wired-rate 30 ● On the AC, set the maximum bandwidth of port 3 on all APs to 30 Mbps. FS(config)# ap-config all FS(config-ap)# wired-rate 30 port 3 ● On the AC, set the maximum bandwidth of port 3 of slot 3 on the i-Share+ AP to 30 Mbps. FS(config)# ap-config am5528 FS(config-ap)# wired-rate 30 port 3 slot 3 ● On the AC, set the maximum bandwidth of all LAN ports of slot 3 on the i-Share+ AP to 30 Mbps.

	FS(config)# ap-config am5528 FS(config-ap)# wired-rate 30 slot 3
AP120-W	● On one AP120-W, set the maximum bandwidth of FastEthernet 0/4 to 40 Mbps. FS(config)#interface fastEthernet 0/4 FS(config-if-FastEthernet 0/4)#wired-rate 40
AP130-W	● On one AP130-W, set the maximum bandwidth of GigabitEthernet 0/4 to 40 Mbps. FS(config)#interface GigabitEthernet 0/4 FS(config-if-GigabitEthernet 0/4)#wired-rate 40
Verification	● On the AC, run the **show ap-config running-config** command to display the configuration.
AC	FS(config)# show ap-config running-config ap-config ap120w-4 wired-rate 30 port 3
	● On the AC, run the **show running-config** command to display the configuration.
AC	FS(config)# show running-config ap-group default wired-rate 30 port 3
	● On the AC, run the **show running-config** command to display the configuration.
AC	FS(config)# show running-config ap-group default wired-rate 30
	● On the AC, run the **show running-config** command to display the configuration.

AC	FS(config)# show running-config ap-config all … wired-rate 30 port 3 … FS(config)# show running-config ap-config am5528 … wired-rate 30 port 3 slot 3 … FS(config)# show running-config ap-config am5528 … wired-rate 30 slot 3 …
	● On the AP, run the **show running-config** command to display the configuration.
AP120-W	FS(config)# show running-config … interface FastEthernet 0/4 wired-rate 40 …
AP130-W	FS(config)# show running-config … interface GigabitEthernet 0/4 wired-rate 40 …

Common Errors

- N/A

5.5 Monitoring

- N/A

6 Configuring DATA-PLANE

6.1 Overview

The data plane provides broadcast forwarding control functions, including broadcast forwarding weight control and broadcast wireless forwarding control.

Broadcast forwarding weight control means restricting the weights of packet types for broadcast forwarding, so as to prevent STAs from being influenced when a certain type of packets occupy all resources.

Broadcast wireless forwarding control means forwarding only necessary packets to the wireless network, so as to prevent some useless broadcast packets from occupying substantial radio frequency (RF) resources.

- Broadcast forwarding weight control is applicable to all packets to be flooded.
- Broadcast wireless forwarding control is applicable to all packets to be sent to the radio interface.

Protocols and Standards

- N/A

6.2 Applications

Application	Description
Broadcast Forwarding Control	Set up the network with at least one AC and one fit AP.

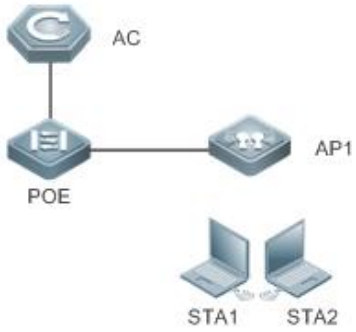
6.2.1 Broadcast Forwarding Control

Scenario

An AC is deployed in the wireless network and enabled with broadcast wireless forwarding control function.

The AC controls the wireless forwarding of broadcast packets, as shown in Figure 6-1.

Figure 6-1



AC: a wireless access controller.

PoE: a gateway switch for the AP.

AP: a wireless access point.

STA1 and STA2: user equipment used as STAs.

Corresponding Protocols

- Enable the broadcast wireless forwarding control function on the AC.

6.3 Features

Basic Concepts

➘ Broadcast Forwarding Weight Control

A network switching device may need to flood broadcast packets, multicast packets, and some unicast packets. A weight can be set for each type of packets to prevent a certain type of broadcast packets from exhausting all broadcast forwarding capabilities, thereby improving STAs' network experience.

➘ Broadcast Wireless Forwarding Control

The broadcast wireless forwarding control function is used to forward only necessary broadcast packets to the wireless network, so as to prevent certain broadcast packets from occupying substantial air interface resources and improve the network rates of STAs.

Overview

Feature	Description
Broadcast Forwarding Weight Control	Restricts the weights of packet types for broadcast forwarding, so as to protect RF resources from being occupied by a certain type of packets and thereby guarantee normal forwarding of other packets.
Broadcast Wireless Forwarding Control	Controls whether to forward broadcast packets to the wireless network, so as to prevent useless broadcast packets from occupying substantial RF resources.

6.3.1 Broadcast Forwarding Weight Control

Broadcast forwarding weight control is used to restrict a certain type of packets, so that the ratio of this type of packets is no greater than the specified weight during broadcast forwarding.

Working Principle

The broadcast forwarding weight control function classifies packets at first into unicast packets, multicast packets, broadcast packets, unknown multicast packets, and unknown unicast packets.

- Classify packets. Packets may be roughly classified into the following types: unicast packets, multicast packets, broadcast packets, unknown multicast packets, and unknown unicast packets.
- Allocate a token bucket to each type of packets, and record the number of packets permitted to pass at this moment.
- According to the configured broadcast forwarding weights, calculate the number of packets permitted to pass within each interval, and adjust the sizes of the token buckets accordingly.
- When a packet arrives, determine the type of the packet and check whether there is any token in the token bucket corresponding to the packet type. If the token bucket contains a token, the packet is permitted to pass; otherwise, the packet is discarded.

6.3.2 Broadcast Wireless Forwarding Control

The broadcast wireless forwarding control function is used to forward only partial packets that affect STAs to the wireless network, so as to prevent useless broadcast packets from occupying substantial air interface resources.

Working Principle

Wireless networks differ from wired networks in performance. In a wireless network, air interface resources are shared by STAs and APs which often becomes a bottleneck for STAs. Meanwhile, they are seized for a long time because broadcast packets are sent at low rates.

In practice, some broadcast packets are useless for STAs. Forwarding these packets to the wireless network will result in fewer air interface resources and worse user experience.

One solution is to classify broadcast packets for forwarding control. Only the packets of specified types are forwarded to the wireless network.

6.4 Configuration

Configuration	Description and Command	
Broadcast Forwarding Weight Control	Optional configuration. Set the weights of packet types for broadcast forwarding.	
	data-plane queue-weight	Configures the weights of packet types for broadcast forwarding on the AC or AP.
	data-plane token	Configures the refresh interval of the broadcast token bucket and bucket-based rate on the AC or AP.
Broadcast Wireless Forwarding Control	Optional configuration. Enable the broadcast wireless forwarding function.	
	data-plane wireless-broadcast	Enables or disables the broadcast wireless forwarding control function on the AC or AP.

6.4.1 Configuring Broadcast Forwarding Weights

Networking Requirements

- You can control the weight of a packet type for forwarding according to actual network conditions, so as to avoid network congestion for sudden traffic spike.

Notes

- N/A

Configuration Steps

Configuring Broadcast Forwarding Weights

- Optional configuration. Run the **data-plane queue-weight** command to configure the broadcast forwarding weights.
- For centralized forwarding, configure this command in the global configuration mode on the AC.
- For local forwarding, configuration this command in the AP configuration mode on the AC.

Command	**data-plane queue-weight** *unicast-packet-weight multicast-packet-weight broadcast-packet-weight unknown-multicast-packet-weight unknown-unicast-packet-weight*
Parameter Description	*unicast-packet-weight*: sets the forwarding weight of unicast packets. The range is from 1 to 100. The default weight is 16. *multicast-packet-weight*: sets the forwarding weight of multicast packets. The range is from 1 to 50. The default weight is 4. *broadcast-packet-weight*: sets the forwarding weight of broadcast packets. The range is from 1 to 50. The default weight is 2. *unknown-multicast-packet-weight*: sets the forwarding weight of unknown multicast packets. The range is from 1 to 25. The default weight is 1. *unknown-unicast-packet-weight*: sets the forwarding weight of unknown unicast packets. The range is from 1 to 25. The default weight is 1.
Defaults	Default weights are applied.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuring Refresh Interval of Broadcast Token Bucket and Bucket-based Rate

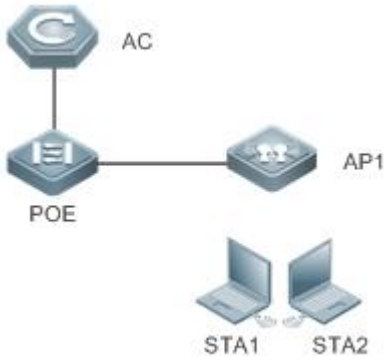
- Optional configuration. Run the **show run** command to display the configuration.
- For centralized forwarding, configure this command in the global configuration mode on the AC.
- For local forwarding, configuration this command in the AP configuration mode on the AC.

Command	**data-plane token** *token-interval token-base-rate*
Parameter Description	*token-interval*: Refresh interval of broadcast token bucket in 10ms. The default interval is 1. *token-base-rate*: Token bucket-based rate. The default rate is 64 for the AC and 5 for the AP.
Defaults	Default parameters are applied.
Command Mode	Global configuration mode
Configuration Usage	Broadcast rate per second = Packet weight × (1s/Refresh Interval) x Token bucket-based rate For example, the broadcast rate per second for the AC = 1 x (1 / 0.01) × 64 = 6400 pps

Configuration Example

Configuring Broadcast Forwarding Weights

Figure 6-2



Configuration Steps	Configure the forwarding weights of packet types for broadcast forwarding in global configuration mode.
AC/AP	FS#configure terminal FS(config)#data-plane queue-weight 100 50 50 25 25 FS(config)#data-plane token 10 10 FS(config)#exit
Verification	Run the **show run** command to display the configuration.
AC/AP	FS#show run … ! cwmp ! data-plane queue-weight 100 50 50 25 25 data-plane token 10 10 ! …

Common Errors

- N/A

6.4.2 Configuring Broadcast Wireless Forwarding

Networking Requirements

- Useless broadcast packets are not forwarded to the air interface.

Notes

- N/A

Configuration Steps

Broadcast Forwarding Function

- Optional configuration. By default, the broadcast wireless forwarding function is disabled. Run the data-plane wireless-broadcast command in global configuration mode to enable or disable this function.

Command	**data-plane wireless-broadcast**{ **enable** | **disable** }
Parameter Description	**enable**: permits all broadcast packets to be forwarded to the air interface **disable**: prohibits all broadcast packets from being forwarded to the air interface
Defaults	The broadcast wireless forwarding function is disabled; that is, broadcast packets are not forwarded to the wireless network.
Command Mode	Global configuration mode
Configuration	N/A

Usage	

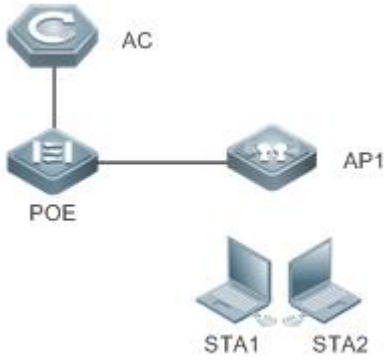
Verification

- Run the show run command to display configuration information.

Configuration Example

Enabling the Broadcast Wireless Forwarding Function

Figure 6-3



Configuration Steps	Enable the broadcast wireless forwarding function in global configuration mode.
AC/AP	FS#configure terminal FS(config)#data-plane wireless-broadcast enable
Verification	Run the **show running-config** command to display the configuration.
AC/AP	FS# show ap-config running ! cwmp ! data-plane wireless-broadcast enable !

Common Errors

- N/A

6.5 Monitoring

- N/A

7 Configuring WLOG

7.1 Overview

WLOG (WLAN Log) enables storing and viewing wireless network and STA status in a past period of time. By collecting and storing the information of wireless network, AP and STA in the past 24 hours and then displaying the information through CLI commands, WLOG allows users to analyze the wireless network status and troubleshoot problems.

WLOG is for collecting and storage information, but does not support automatic information analysis temporarily. The WLOG feature is dedicated to enabling users, with provided information, to have a more accurate understanding of the wireless network and STA status in the past 24 hours to analyze and troubleshoot problems.

There are two types of WLOG information storage: storage on AC and storage on AP. Currently, all information is stored on AC except "STA's Spatial Information" which is stored on AP.

Protocols and Standards

- N/A

7.2 Applications

Application	Description
Fit AP Networking	The fit AP networking includes at least one AC and one AP.

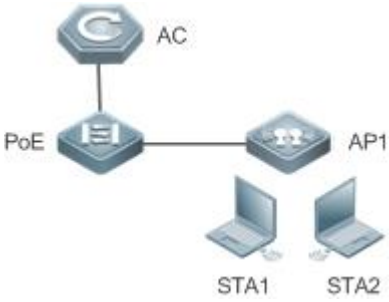
7.2.1 Fit AP Networking

Scenario

Deploy an AC device in a wireless network to query the information on the whole network, AP and STA associated with the AC device.

Figure 7-1 shows the networking topology for viewing the information on the whole network, AP and STA associated with the AC device.

Figure 7-1



Note:	AC: wireless controller PoE: switch, acted as the gateway of the AP AP: wireless access device STA1 and STA2: user devices, used as STA

Deployment

- Enable the WLOG feature on an AC device.

7.3 Features

Basic Concepts

Two Modes of Information Collection on the AC

- Periodic Collection

The general information of the whole network, AP and STA is collected and stored on a regular basis (once/1 hour). The general AP and STA information covers all the information of online APs and STAs.

- Reception Advertisement Collection

When an AP behavior of "AP Behavior Type" occurs, the WLOG module is informed to collect and store the information of the behavior.

When a STA behavior of "STA Behavior Type" occurs, the WLOG module is informed to collect and store the information of the behavior.

The information collection on the AP covers only periodic collection of spatial information on all online STAs.

General Information on the Whole Network

- Continuous operation time of the AC
- Number of online APs
- Number of preset but offline APs
- Versions of online APs (number of APs of each version)
- The information on each WLAN (SSID) STA includes:
- Number of online STAs which have passed Web authentication
- Number of online STAs which have passed 802.1x authentication
- Number of online STAs which are authentication-free

General Information on the AP

- AP name
- AP MAC address
- AP IP address
- AP uptime
- Status of each wired port of the AP
- Input/output rate (bits/sec) in last 5 minutes
- Statistics of input/output of unicast, broadcast, multicast and error frames
- General information on each radio
- Working channel
- Transmit power (dBm, absolute value)
- Number of associated online STAs
- Number of online STAs which have passed Web authentication

- Number of online STAs which have passed 802.1x authentication
- Intensity of the co-channel interference signal
- Number of received error frames
- Packet retransmission times

General Information on the STA

- IP address
- Signal strength
- Access rate
- Associated AP, radio and SSID

STA's Spatial Information

- The STA's spatial information mainly includes the statistics of data frame and management frame of the STA, as well as the statistics of each type of rate, as detailed below:
- Number of data frames successfully transmitted (from the AP to the STA)/total traffic
- Number of unresponsive data frames/total traffic
- Number of management frames/total traffic
- Statistics of each type of frames with access rate (The access rate is divided into 8 grades for statistics)

Grade	0	1	2	3	4	5	6	7
Access Type (Mbps)	1/2	5.5/11	6/9	12/18	24/36	48/54	Reserved	Reserved

- Statistics of each type of frame with MIMO rate (The MIMO rate is divided into 8 grades for statistics)

Grade	0	1	2	3	4	5	6	7
MIMO Type	mcs0 mcs1	mcs2 mcs3	mcs4 mcs5	mcs6 mcs7	mcs8 mcs9	mcs10 mcs11	mcs12 mcs13	mcs14 mcs15

The spatial information is mainly used to check whether the STA is in low-speed state, whether the proportion of the case in which no ACK frame is transmitted is too high, and whether too many management frames are transmitted and received, so as to further analyze and locate the network problems caused by low speed node, management frame attack, and poor condition. The STA's spatial information varies in real time, and the current collection frequency is once every five minutes. The information is saved only on the AP due to large data volume.

AP Behavior Type

The AP behavior type includes going online, going offline and CAPWAP connection failure.

STA Behavior Type

The STA behavior type includes: association, de-association, Web authentication going online, Web authentication offline, 802.1X authentication going online, and 802.1X authentication offline.

Features

Feature	Description

Enabling the WLOG Feature	You can enable the WLOG feature to automatically collect AC, AP and STA information.
Synchronizing STA Go-online/offline Information to the ELOG Server	Synchronize STA go-online/offline information to the ELOG server.

7.3.1 Enabling the WLOG Feature

After the WLOG feature is enabled, the AC or AP automatically collects AC, AP and STA information and records the information into memory, enabling users, with provided information, to have a more accurate understanding of the wireless network and STA status in the past 24 hours and analyze and troubleshoot problems.

Working Principle

After the WLOG feature is enabled, the AC or AP automatically collects AC, AP and STA information and records the information into memory, and receives online/offline advertisement of the AP and STA and records into memory for users to view.

7.3.2 Synchronizing STA Go-online/offline Information to the ELOG Server

After the WLOG function is enabled and the ELOG server URL is configured, the AC sends STA information to the ELOG server when a STA goes online or offline.

Working Principle

After the WLOG function is enabled and the AC receives the STA go-online/offline notice, the AC sends STA information in a specific format to the ELOG server.

7.4 Configuration

Configuration	Description and Command	
Enabling the WLOG Feature	(Mandatory) It is used to enable the WLOG feature.	
	wlan diag enable	Enables the WLOG feature
Synchronizing STA Go-online/offline Information to the ELOG Server	(Optional) It is used to synchronize STA go-online/offline information to the ELOG server.	
	web-server enable api-path assoc-sta url *url*	Configures the address of the ELOG server.

7.4.1 Enabling the WLOG Feature

Configuration Effect

- After the WLOG feature is enabled, the AC or AP automatically records the AC, AP and STA information.

Notes

- Enabling the WLOG feature pre-allocates memory. If the memory is not sufficient, the WLOG feature cannot be enabled. Disabling the WLOG feature frees all memory for information storage and pre-allocated memory.

Configuration Steps

Enabling the WLOG Feature

- (Mandatory) Run the **wlog diag enable** command to enable the WLOG feature.

- Enable the WLOG feature in global configuration mode of the AC device.
- After the WLOG feature is enabled, information is collected and recorded into memory on a regular basis.

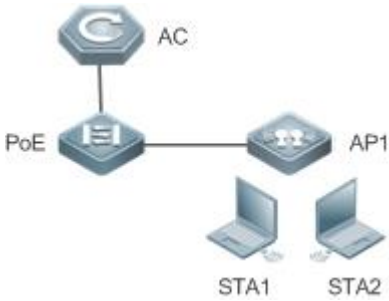
Command	**wlan diag enable**
Parameter Description	N/A
Defaults	By default, the WLOG feature is disabled on the AC and AP device.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show wlan diag network** command to check whether the whole network information can be viewed on the AC.
- Run the **show wlan diag sta** command to check whether the STA information can be viewed on the AP.

Configuration Example

Enabling the WLOG Feature

Scenario **Figure 7-2**	
Configuration Steps	● Enable the WLOG feature in global configuration mode.
AC	FS# configure terminal FS(config)# wlan diag enable
Verification	Use the **show wlan diag network** command to display the general information of the whole network.
AC	FS# show wlan diag network Time: 2013-10-20 16:44:45 AC uptime: 294 h Online AP: 1 Offline AP:0 Online AP Version: PID HwVer SwVer AP Number --- --- --- --- AAP320-I 1.00 FSOS 10.4(1b19)p2, Release(167368) 1 Wlan information:

	WSSID Active STA WEB Auth 1X Auth Open 4---------- ---------- -------- -------- -------- GWLAN_1T13_wireless 0 0 5 0 1 FSWLAN_IT13_wireless_1X 0 0 0 0 guest_only 0 0 0 1

7.4.2 Synchronizing STA Go-online/offline Information to the ELOG Server

Configuration Effect

- After the WLOG function is enabled and the ELOG server URL is configured, the AC sends the STA go-online/offline information to the ELOG server.

Notes

- This function is triggered by the STA go-online/offline action. Before the function is enabled, the STA go-online/offline information is not sent to the ELOG server.

Configuration Steps

Configuring the URL of the ELOG Server

- The complete address of the ELOG server needs to be configured.

Command	**web-server enable api-path assoc-sta url** *url*
Parameter Description	*url*: indicates the complete address of the ELOG server.
Defaults	By default, The ELOG server URL is not configured, that is, the AC does not interwork with the ELOG server.
Command Mode	Global configuration mode
Usage Guide	To ensure smooth data transmission, the WLOG function needs to be enabled. In local forwarding scenarios, if the AC does not obtain the STA IP address (which can be queried by running the **show ac-config client** command) after the STA goes online, run the **ip dhcp snooping** command in global configuration mode to ensure that the AC can obtain the STA IP address.

Verification

- Run the **show running** command to display configurations.

Configuration Example

Configuring the URL of the ELOG Server

Configuration Steps	• In global configuration mode, configure the Elog server URL.
AC	FS# configure terminal FS(config)#web-server enable api-path assoc-sta url http://172.18.155.14:8080/elog/service/dc/updateSta
Verification	Run the **show running-config** command to display configurations.
AC	FS# show running-config

	! web-server enable api-path assoc-sta url http://172.18.155.14:8080/elog/service/dc/updateSta http://172.18.155.14:8080/elog/service/dc/updateSta

Common Errors

- Only an IP address instead of a complete URL is specified in the URL parameter.

Common Errors

- N/A

7.5 Monitoring

Displaying

Description	Command
Displays the general information on the whole network	**show wlan diag network**
Displays the AP information on the AC	**show wlan diag ap** [**ap-mac** *ap-mac*] [**number** *number*]
Displays the STA information on the AC	**show wlan diag sta** [**sta-mac** *sta-mac*] [**ip-range** *ip-prefix*] [**action** *action* [**result** *result*]] [**number** *number*]

Chapter 16 Interface Configuration

1. Configuring Interfaces
2. Configuring MODE-MGMT
3. Configuring DLDP
4. Configuring PCAP
5. Configuring PPPoE-CLIENT
6. Configuring PPPoE-SERVER
7. Configuring Aggregated Port
8. Configuring VLAN-TERMINAL

1 Configuring Interfaces

1.1 Overview

Interfaces are important in implementing data switching on network devices. FS devices support two types of interfaces: physical ports and logical interfaces. A physical port is a hardware port on a device, such as the 100M Ethernet interface and gigabit Ethernet interface. A logical interface is not a hardware port on the device. A logical interface, such as the loopback interface and tunnel interface, can be associated with a physical port or independent of any physical port. For network protocols, physical ports and logical interfaces serve the same function.

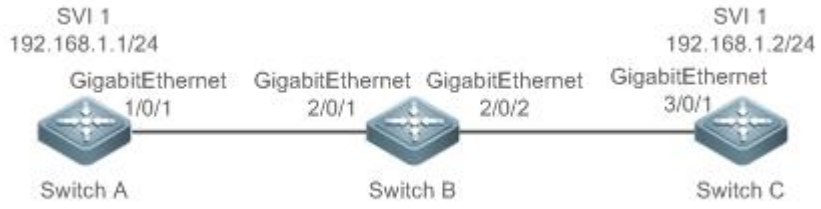
1.2 Applications

Application	Description
L2 Data Switching Through the Physical Ethernet Interface	Implement Layer-2 (L2) data communication of network devices through the physical L2 Ethernet interface.
L3 Routing Through the Physical Ethernet Interface	Implement Layer-3 (L3) data communication of network devices through the physical L3 Ethernet interface.

1.2.1 L2 Data Switching Through the Physical Ethernet Interface

Scenario

Figure 1- 1



As shown in Figure 1- 1 , Switch A, Switch B, and Switch C form a simple L2 data switching network.

Deployment

- Connect Switch A to Switch B through physical ports GigabitEthernet 1/0/1 and GigabitEthernet 2/0/1.
- Connect Switch B to Switch C through physical ports GigabitEthernet 2/0/2 and GigabitEthernet 3/0/1.
- Configure GigabitEthernet 1/0/1, GigabitEthernet 2/0/1, GigabitEthernet 2/0/2, and GigabitEthernet3/0/1 as Trunk ports.
- Create a switch virtual interface (SVI), SVI 1, on Switch A and Switch C respectively, and configure IP addresses from a network segment for the two SVIs. The IP address of SVI 1 on Switch A is 192.168.1.1/24, and the IP address of SVI 1 on Switch C is 192.168.1.2/24.
- Run the **ping 192.168.1.2** command on Switch A and the **ping 192.168.1.1** command on Switch C to implement data switching through Switch B.

1.2.2 L3 Routing Through the Physical Ethernet Interface

Scenario

Figure 1- 2

As shown in Figure 1- 2, Switch A, Switch B, and Switch C form a simple L3 data communication network.

Deployment

- Connect Switch A to Switch B through physical ports GigabitEthernet 1/0/1 and GigabitEthernet 2/0/1.
- Connect Switch B to Switch C through physical ports GigabitEthernet 2/0/2 and GigabitEthernet 3/0/1.
- Configure GigabitEthernet 1/0/1, GigabitEthernet 2/0/1, GigabitEthernet 2/0/2, and GigabitEthernet3/0/1 as L3 routed ports.
- Configure IP addresses from a network segment for GigabitEthernet 1/0/1 and GigabitEthernet 2/0/1. The IP address of GigabitEthernet 1/0/1 is 192.168.1.1/24, and the IP address of GigabitEthernet 2/0/1 is 192.168.1.2/24.
- Configure IP addresses from a network segment for GigabitEthernet 2/0/2 and GigabitEthernet 3/0/1. The IP address of GigabitEthernet 2/0/2 is 192.168.2.1/24, and the IP address of GigabitEthernet 3/0/1 is 192.168.2.2/24.
- Configure a static route entry on Switch C so that Switch C can directly access the network segment 192.168.1.0/24. Configure a static route entry on Switch A so that Switch A can directly access the network segment 192.168.2.0/24
- Run the **ping 192.168.2.2** command on Switch A and the **ping 192.168.1.1** command on Switch C to implement L3 routing through Switch B.

1.3 Features

Basic Concepts

Interface Classification

Interfaces on FS devices fall into three categories:

- L2 interface (Switch or bridge mode)
- L3 interface (supported by L3 devices)

9. Common L2 interfaces are classified into the following types:

- Switch port
- L2 aggregate port (AP)

10. Common L3 interfaces are classified into the following types:

- Routed port
- L3 AP port
- Loopback interface
- Tunnel interface

Switch Port

A switch port is an individual physical port on the device, and implements only the L2 switching function. The switch port is used to manage physical ports and L2 protocols related to physical ports.

L2 AP Port

An AP port is formed by aggregating multiple physical ports. Multiple physical links can be bound together to form a simple logical link. This logical link is called an AP port.

For L2 switching, an AP port is equivalent to a switch port that combines bandwidths of multiple ports, thus expanding the link bandwidth. Frames sent over the L2 AP port are balanced among the L2 AP member ports. If one member link fails, the L2 AP port automatically transfers the traffic on the faulty link to other member links, improving reliability of connections.

Routed Port

A physical port on a L3 device can be configured as a routed port, which functions as the gateway interface for L3 switching. A routed port is not related with a specific VLAN. Instead, it is just an access port. The routed port cannot be used for L2 switching.

.

L3 AP Port

Like the L2 AP port, a L3 AP port is a logical port that aggregates multiple physical member ports. The aggregated ports must be the L3 ports of the same type. The AP port functions as a gateway interface for L3 switching. Multiple physical links are combined into one logical link, expanding the bandwidth of a link. Frames sent over the L3 AP port are balanced among the L3 AP member ports. If one member link fails, the L3 AP port automatically transfers the traffic on the faulty link to other member links, improving reliability of connections.

Loopback Interface

The loopback interface is a local L3 logical interface simulated by the software that is always UP. Packets sent to the loopback interface are processed on the device locally, including the route information. The IP address of the loopback interface can be used as the device ID of the Open Shortest Path First (OSPF) routing protocol, or as the source address used by Border Gateway Protocol (BGP) to set up a TCP connection. The procedure for configuring a loopback interface is similar to that for configuring an Ethernet interface, and you can treat the loopback interface as a virtual Ethernet interface.

Tunnel Interface

The Tunnel interface implements the tunnel function. Over the Tunnel interface, transmission protocols (e.g., IP) can be used to transmit packets of any protocol. Like other logical interfaces, the tunnel interface is also a virtual interface of the system. Instead of specifying any transmission protocol or load protocol, the tunnel interface provides a standard point-to-point (P2P) transmission mode. Therefore, a tunnel interface must be configured for every individual link.

Overview

Feature	Description
Interface Configuration Commands	You can configure interface-related attributes in interface configuration mode. If you enter interface configuration mode of a non-existing logical interface, the interface will be created.
Interface Description and Administrative Status	You can configure a name for an interface to identify the interface and help you remember the functions of the interface. You can also configure the administrative status of the interface.
MTU	You can configure the maximum transmission unit (MTU) of a port to limit the length of a frame that can be received or sent over this port.
Bandwidth	You can configure the bandwidth of an interface.
Load Interval	You can specify the interval for load calculation of an interface.
Carrier Delay	You can configure the carrier delay of an interface to adjust the delay after which the status of an interface changes from Down to Up or from Up to Down.
Link Trap Policy	You can enable or disable the link trap function on an interface.
Interface Index Persistence	You can enable the interface index persistence function so that the interface index remains unchanged after the device is restarted.
Selection of Interface Medium Type	You can select the medium type (fiber or copper) of a combo port as required.
Interface Speed, Duplex Mode, Flow Control Mode, and Auto Negotiation Mode	You can configure the speed, duplex mode, flow control mode, and auto negotiation mode of an interface.

Feature	Description
Automatic Module Detection	If the interface speed is set to auto, the interface speed can be automatically adjusted based on the type of the inserted module.
Port Flapping Protection	You can configure the port flapping protection function so that the system can automatically shut down a port when flapping occurs on the port.

1.3.1 Interface Configuration Commands

üRun the interface command in global configuration mode to enter interface configuration mode. You can configure interface-related attributes in interface configuration mode.

Working Principle

Run the interface command in global configuration mode to enter interface configuration mode. If you enter interface configuration mode of a non-existing logical interface, the interface will be created. You can also run the interface range or interface range macro command in global configuration mode to configure the range (IDs) of interfaces. Interfaces defined in the same range must be of the same type and have the same features.

You can run the **no interface** command in global configuration mode to delete a specified logical interface.

Interface Numbering Rules

In stand-alone mode, the ID of a physical port consists of two parts: slot ID and port ID on the slot. For example, if the slot ID of the port is 2, and port ID on the slot is 3, the interface ID is 2/3. In VSU or stack mode, the ID of a physical port consists of three parts: device ID, slot ID, and port ID on the slot. For example, if the device ID is 1, slot ID of the port is 2, and port ID on the slot is 3, the interface ID is 1/2/3.

The device ID ranges from 1 to the maximum number of supported member devices.

The slot number rules are as follows: The static slot ID is 0, whereas the ID of a dynamic slot (pluggable module or line card) ranges from 1 to the number of slots. Assume that you are facing the device panel. Dynamic slot are numbered from 1 sequentially from front to rear, from left to right, and from top to bottom.

The ID of a port on the slot ranges from 1 to the number of ports on the slot, and is numbered sequentially from left to right.

You can select fiber or copper as the medium of a combo port. Regardless of the medium selected, the combo port uses the same port ID.

The ID of an AP port ranges from 1 to the number of AP ports supported by the device.

The ID of an SVI is the VID of the VLAN corresponding to this SVI.

Configuring Interfaces Within a Range

You can run the **interface range** command in global configuration mode to configure multiple interfaces at a time. Attributes configured in interface configuration mode apply to all these interfaces.

The **interface range** command can be used to specify several interface ranges.

The **macro** parameter is used to configure the macro corresponding to a range. For details, see "Configuring Macros of Interface Ranges."

Ranges can be separated by commas (,).

The types of interfaces within all ranges specified in a command must be the same.

Pay attention to the format of the **range** parameter when you run the **interface range** command.

The following interface range formats are valid:

- **FastEthernet** device/slot/{first port} - {last port};
- **GigabitEthernet** device/slot/{first port} - {last port};
- **TenGigabitEthernet** device/slot/{first port} - {last port};
- **FortyGigabitEthernet** device/slot/{first port} - {last port};
- **AggregatePort** *Aggregate-port ID* (The AP ID ranges from 1 to the maximum number of AP ports supported by the device.)

- **Loopback** loopback-ID (The loopback ID ranges from 1 to 2,147,483,647.)
- **Tunnel** tunnel-ID (The tunnel ID ranges from 0 to the maximum number of tunnel interfaces supported by the device minus 1.)

Interfaces in an interface range must be of the same type, namely, FastEthernet, GigabitEthernet, AggregatePort, or SVI.

Configuring Macros of Interface Ranges

You can define some macros to replace the interface ranges. Before using the **macro** parameter in the **interface range** command, you must first run the **define interface-range** command in global configuration mode to define these macros.

Run the **no define interface-range macro_name** command in global configuration mode to delete the configured macros.

1.3.2 Interface Description and Administrative Status

You can configure a name for an interface to identify the interface and help you remember the functions of the interface.

You can enter interface configuration mode to enable or disable an interface.

Working Principle

Interface Description

You can configure the name of an interface based on the purpose of the interface. For example, if you want to assign GigabitEthernet 1/1 for exclusive use by user A, you can describe the interface as "Port for User A."

Interface Administrative Status

You can configure the administrative status of an interface to disable the interface as required. If the interface is disabled, no frame will be received or sent on this interface, and the interface will loss all its functions. You can enable a disabled interface by configuring the administrative status of the interface. Two types of interface administrative status are defined: Up and Down. The administrative status of an interface is Down when the interface is disabled, and Up when the interface is enabled.

1.3.3 MTU

You can configure the MTU of a port to limit the length of a frame that can be received or sent over this port.

Working Principle

When a large amount of data is exchanged over a port, frames greater than the standard Ethernet frame may exist. This type of frame is called jumbo frame. The MTU is the length of the valid data segment in a frame. It does not include the Ethernet encapsulation overhead. If a port receives or sends a frame with a length greater than the MTU, this frame will be discarded.

1.3.4 Bandwidth

Working Principle

The **bandwidth** command can be configured so that some routing protocols (for example, OSPF) can calculate the route metric and the Resource Reservation Protocol (RSVP) can calculate the reserved bandwidth. Modifying the interface bandwidth will not affect the data transmission rate of the physical port.

The **bandwidth** command is a routing parameter, and does not affect the bandwidth of a physical link.

1.3.5 Load Interval

Working Principle

You can run the **load-interval** command to specify the interval for load calculation of an interface. Generally, the interval is 10s.

1.3.6 Carrier Delay

Working Principle

The carrier delay refers to the delay after which the data carrier detect (DCD) signal changes from Down to Up or from Up to Down. If the DCD status changes during the delay, the system will ignore this change to avoid negotiation at the upper data link layer. If this parameter is set to a great value, nearly every DCD change is not detected. On the contrary, if the parameter is set to 0, every DCD signal change will be detected, resulting in poor stability.

If the DCD carrier is interrupted for a long time, the carrier delay should be set to a smaller value to accelerate convergence of the topology or route. On the contrary, if the DCD carrier interruption time is shorter than the topology or route convergence time, the carrier delay should be set to a greater value to avoid topology or route flapping.

1.3.7 Link Trap Policy

You can enable or disable the link trap function on an interface.

Working Principle

When the link trap function on an interface is enabled, the Simple Network Management Protocol (SNMP) sends link traps when the link status changes on the interface.

1.3.8 Interface Index Persistence

Like the interface name, the interface index also identifies an interface. When an interface is created, the system automatically assigns a unique index to the interface. The index of an interface may change after the device is restarted. You can enable the interface index persistence function so that the interface index remains unchanged after the device is restarted.

Working Principle

After interface index persistence is enabled, the interface index remains unchanged after the device is restarted.

1.3.9 Selection of Interface Medium Type

You can select the medium type (fiber or copper) of a combo port as required.

Working Principle

You can choose either fiber or copper as the medium, but the two media cannot take effect at the same time. Once you select the medium, attributes, including the connection status, speed, duplex mode, and flow control mode, are attributes of the selected medium. If you change the medium, the interface will adopt the default settings, and you must re-configure these attributes according to requirements.

The Combo Port Supports Automatic Selection of the Medium Type

- If you enable automatic selection of the medium type, the device uses the current medium if only one medium is available.
- If both media are available, the device uses the preferred medium that is configured. By default, the preferred medium is copper.

You can run the **medium-type auto-select prefer fiber** command to configure fiber as the preferred media. In automatic medium selection mode, the interface adopts the default settings of attributes, such as the speed, duplex mode, and flow control mode.

If an interface is enabled with automatic selection, its peer interface must be enabled with auto negotiation; otherwise, an error will occur.

The command takes effect only on a physical port. An AP port or SVI does not support configuration of the medium type.

The command takes effect only on a port that supports medium selection.

All ports that are configured as member ports of an AP port must have the same medium type; otherwise, they cannot be added to the AP port. The type of member ports cannot be modified. A port enabled with automatic medium selection cannot be added to an AP port.

1.3.10 Interface Speed, Duplex Mode, Flow Control Mode, and Auto Negotiation Mode

You can configure the interface speed, duplex mode, flow control mode, and auto negotiation mode of an Ethernet physical port or AP port.

Working Principle

Speed

Generally, the speed of an Ethernet physical port is determined through negotiation with the peer device. The negotiated speed can be any speed within the interface capability. You can also configure any speed within the interface capability for the Ethernet physical port. When you configure the speed of an AP port, the configuration takes effect on all of its member ports. (All these member ports are Ethernet physical ports.)

Duplex Mode

- The duplex mode of an Ethernet physical port or AP port can be configured as follows:
- Set the duplex mode of the interface to full-duplex so that the interface can receive packets while sending packets.
- Set the duplex mode of the interface to half-duplex so that the interface can receive or send packets at a time.
- Set the duplex mode of the interface to auto-negotiation so that the duplex mode of the interface is determined through auto negotiation between the local interface and peer interface.
- When you configure the duplex mode of an AP port, the configuration takes effect on all of its member ports. (All these member ports are Ethernet physical ports.)

1.3.11 Automatic Module Detection

If the interface speed is set to auto, the interface speed can be automatically adjusted based on the type of the inserted module.

Working Principle

Currently, the automatic module detection function can be used to detect only the SFP and SFP+ modules. The SFP is a Gigabit module, whereas SFP+ is a 10 Gigabit module. If the inserted module is SFP, the interface works in Gigabit mode. If the inserted module is SFP+, the interface works in 10 Gigabit mode.

The automatic module detection function takes effect only when the interface speed is set to auto.

1.3.12 Port Flapping Protection

When flapping occurs on a port, a lot of hardware interruptions occur, consuming a lot of CPU resources. On the other hand, frequent port flapping damages the port. You can configure the flapping protection function to protect ports.

Working Principle

By default, the port flapping protection function is enabled. You can disable this function as required. When flapping occurs on a port, the port detects flapping every 2s or 10s. If flapping occurs six times within 2s on a port, the device displays a prompt. If 10 prompts are displayed continuously, that is, port flapping is detected continuously within 20s, the port is disabled. If flapping occurs 10 times within 10s on a port, the device displays a prompt without disabling the port.

1.3.13 Syslog

You can enable or disable the syslog function to determine whether to display information about the interface changes or exceptions.

Working Principle

You can enable or disable the syslog function as required. By default, this function is enabled. When an interface becomes abnormal, for example, the interface status changes, or the interface receives error frames, or flapping occurs, the system displays prompts to notify users.

1.3.14 Interface MAC Address

Working Principle

By default, each Ethernet interface has a globally unique MAC address. The MAC addresses of Ethernet interfaces can be modified if required. However, MAC addresses in the same LAN must be unique.

To configure the MAC address of an Ethernet interface, run the **mac-address** command in interface configuration mode:

Configuration of MAC addresses may affect internal communication in a LAN. Therefore, it is recommended that users do not configure MAC addresses by themselves if unnecessary.

Related Configuration

Configuring MAC Addresses for Interfaces

By default, each interface has a globally unique MAC address.

You can run the **mac-address** ***mac-address*** command in interface configuration mode to modify the MAC address of an interface.

1.3.15 VLAN Encapsulation Flag on Interfaces

Working Principle

Virtual local area network (VLAN) is a logical network divided on a physical network and corresponds to the layer-2 network in the ISO model. In 1999, IEEE released the 802.1Q protocol draft for standardizing the VLAN implementation solution.

The VLAN technology enables the network administrator to divide a physical LAN into multiple broadcast domains (or VLANs). Each VLAN contains a group of workstations with the same requirements and each VLAN has the same attributes as the physical LAN.As VLANs are logically divided, workstations in the same VLAN do not need to be placed in the same physical space, that is, these workstations may belong to different physical LAN network segments. Multicast and unicast traffic in a VLAN will not be forwarded to other VLANs. This helps control traffic, reduce device investment, simplify network management, and improve the network security.

VLAN is a protocol used to solve Ethernet broadcast and security problems. During packet transmission, a VLAN header is added to Ethernet frames. In addition, VLAN IDs are used to classify users to different work groups to restrict layer-2 exchange between users in different work groups. Each work group is a VLAN.VLANs can be used to restrict the broadcast scope and form virtual work groups to manage networks dynamically.

To ensure communication with hosts in a VLAN, users can configure the 802.1Q (VLAN protocol) VLAN encapsulation flag on the Ethernet interface or sub-interface. In this case, when packets are sent over the Ethernet interface, the corresponding VLAN header will be encapsulated. When packets are received, the VLAN header will be deleted from the packet.

Related Configuration

Configuring the VLAN Encapsulation Flag for Interfaces

By default, the 802.1Q encapsulation protocol is disabled for interfaces.

You can run the **encapsulation dot1Q VlanID** command in interface mode for 802.1Q encapsulation for an interface. **VlanID** indicates the encapsulated VLAN ID.

1.3.16 Keepalive Packet Period

Working Principle

On common WAN interfaces, the encapsulated link layer protocol requires the keepalive mechanism to ensure proper working. By configuring the keepalive function, the keepalive period of the link layer protocol can be set, to control the interval for sending keepalive packets.

On tunnel interfaces and interfaces with the HDLC or PPP protocol for encapsulation, the maximum number of timeouts of keepalive packets can be set. If no response is received from the peer end after the maximum number of timeouts of a keepalive packet is reached, the connection is disconnected.

Related Configuration

Configuring the Keepalive Packet Period for Interfaces

By default, the keepalive function is disabled on Ethernet interfaces. The default keepalive packet period on other interfaces is 10s, and the value range of the keepalive packet period is from 1 to 32767 in seconds.

On tunnel interfaces and interfaces with the HDLC or PPP protocol for encapsulation, the keepalive command also carries the maximum number of timeouts of keepalive packets. The value range is from 1 to 255. By default, the maximum number of keepalive packet timeouts on tunnel interfaces, HDLC interfaces, and PPP interfaces are 3, 3, and 10, respectively.

You can run the keepalive [keep-period [keep-retries]] command in interface configuration mode to change the keepalive packet period for an interface.

1.4 Configuration

Configuration	Description and Command	
Performing Basic Configurations	(Optional) It is used to manage interface configurations, for example, creating/deleting an interface, or configuring the interface description.	
	interface	Creates an interface and enters configuration mode of the created interface or a specified interface.
	interface range	Enters an interface range, creates these interfaces (if not created), and enters interface configuration mode.
	define interface-range	Creates a macro to specify an interface range.
	snmp-server if-index persist	Enables the interface index persistence function so that the interface index remains unchanged after the device is restarted.
	description	Configures the interface description of up to 80 characters in interface configuration mode.
	snmp trap link-status	Configures whether to send the link traps of the interface.
	shutdown	Shuts down an interface in interface configuration mode.

1.4.1 Performing Basic Configurations

Configuration Effect

- Create a specified logical interface and enter configuration mode of this interface, or enter configuration mode of an existing physical or logical interface.
- Create multiple specified logical interfaces and enter interface configuration mode, or enter configuration mode of multiple existing physical or logical interfaces.
- The interface indexes remain unchanged after the device is restarted.

- Configure the interface description so that users can directly learn information about the interface.
- Enable or disable the link trap function of an interface.
- Enable or disable an interface.

Notes

- The **no** form of the command can be used to delete a specified logical interface or logical interfaces in a specified range, but cannot be used to delete a physical port or physical ports in a specified range.
- The **default** form of the command can be used in interface configuration mode to restore default settings of a specified physical or logical interface, or interfaces in a specified range.

Configuration Steps

Configuring a Specified Interface

- Optional.
- Run this command to create a logical interface or enter configuration mode of a physical port or an existing logical interface.

Command	**interface** *interface-type interface-number*
Parameter Description	*interface-type interface-number*: Indicates the type and number of the interface. The interface can be an Ethernet physical port, AP port, SVI, or loopback interface.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	● If a logical interface is not created yet, run this command to create this interface and enter configuration mode of this interface. ● For a physical port or an existing logical interface, run this command to enter configuration mode of this interface. ● Use the **no** form of the command to delete a specified logical interface. ● Use the **default** form of the command to restore default settings of the interface in interface configuration mode.

Configuring Interfaces Within a Range

- Optional.
- Run this command to create multiple logical interfaces or enter configuration mode of multiple physical port or existing logical interfaces.

Command	**interface range** { *port-range* | **macro** *macro_name* }
Parameter Description	*port-range*: Indicates the type and ID range of interfaces. These interfaces can be Ethernet physical ports, AP ports, SVIs, or loopback interfaces. *macro_name*: Indicates the name of the interface range macro.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	● If logical interfaces are not created yet, run this command to create these interfaces and enter interface configuration mode. ● For multiple physical ports or existing logical interfaces, run this command to enter interface configuration mode. ● Use the **default** form of the command to restore default settings of these interfaces in interface configuration mode.

	● Before using a macro, run the **define interface-range** command to define the interface range as a macro name in global configuration mode, and then run the **interface range macro** *macro_name* command to apply the macro.

Configuring Interface Index Persistence

- Optional.
- Run this command when the interface indexes must remain unchanged after the device is restarted.

Command	**snmp-server if-index persist**
Parameter Description	N/A
Defaults	By default, interface index persistence is disabled.
Command Mode	Global configuration mode
Usage Guide	After this command is executed, current indexes of all interfaces will be saved, and the indexes remain unchanged after the device is restarted. You can use the **no** or **default** form of the command to disable the interface index persistence function.

Configuring the Description of an Interface

- Optional.
- Run this command to configure the description of an interface.

Command	**description** *string*
Parameter Description	*string:* Indicates a string of up to 80 characters.
Defaults	By default, no description is configured.
Command Mode	Interface configuration mode
Usage Guide	This command is used to configure the description of an interface. You can use the **no** or **default** form of the command to delete the description of an interface.-

Configuring the Link Trap Function of an Interface

- Optional.
- Run this command to obtain the link traps through SNMP.

Command	**snmp trap link-status**
Parameter Description	N/A
Defaults	By default, the link trap function is enabled.
Command Mode	Interface configuration mode
Usage Guide	This command is used to configure the link trap function on an interface. When this function is enabled, the SNMP sends link traps when the link status changes on the interface. You can use the **no** or **default** form of the command to disable the link trap function.

Configuring the Administrative Status of an Interface

- Optional.
- Run this command to enable or disable an interface.
- An interface cannot send or receive packets after it is disabled.

Command	**Shutdown**

Parameter Description	N/A
Defaults	By default, the administrative status of an interface is Up.
Command Mode	Interface configuration mode
Usage Guide	You can run the **shutdown** command to disable an interface, or the **no shutdown** command to enable an interface. In some cases, for example, when an interface is in errdisable state, you cannot run the **no shutdown** command on an interface. You can use the **no** or **default** form of the command to enable the interface.

Configuring Port Flapping Protection

- Optional.
- Run this command to protect the port against flapping.

Command	**physical-port dither protect**
Parameter Description	N/A
Defaults	By default, port flapping protection is enabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Syslog Function

- Optional.
- Run this command to enable or disable the syslog function on an interface.

Command	**[no] logging [link-updown | error-frame | link-dither]**
Parameter Description	N/A
Defaults	By default, the syslog function is enabled on an interface.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

Configuring a Specified Interface

- Run the **interface** command. If you can enter interface configuration mode, the configuration is successful.
- For a logical interface, after the **no interface** command is executed, run the **show running** or **show interfaces** command to check whether the logical interface exists. If not, the logical interface is deleted.
- After the **default interface** command is executed, run the **show running** command to check whether the default settings of the corresponding interface are restored. If yes, the operation is successful.

Configuring Interfaces Within a Range

- Run the **interface range** command. If you can enter interface configuration mode, the configuration is successful.
- After the **default interface range** command is executed, run the **show running** command to check whether the default settings of the corresponding interfaces are restored. If yes, the operation is successful.

Configuring Interface Index Persistence

- After the **snmp-server if-index persist** command is executed, run the **write** command to save the configuration, restart the device, and run the **show interface** command to check the interface index. If the index of an interface remains the same after the restart, interface index persistence is enabled.

Configuring the Link Trap Function of an Interface

- Remove and then insert the network cable on a physical port, and enable the SNMP server. If the SNMP server receives link traps, the link trap function is enabled.
- Run the **no** form of the **snmp trap link-status** command. Remove and then insert the network cable on a physical port. If the SNMP server does not receive link traps, the link trap function is disabled.

Configuring the Administrative Status of an Interface

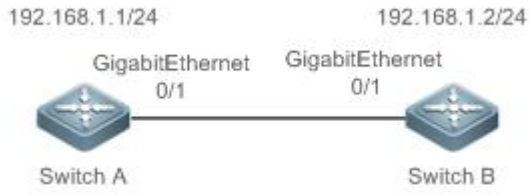
- Insert the network cable on a physical port, enable the port, and run the **shutdown** command on this port. If the syslog is displayed on the Console indicating that the state of the port changes to Down, and the indicator on the port is off, the port is disabled. Run the **show interfaces** command, and verify that the interface state changes to Administratively Down. Then, run the **no shutdown** command to enable the port. If the syslog is displayed on the Console indicating that the state of the port changes to Up, and the indicator on the port is on, the port is enabled.

Configuring Port Flapping Protection

- Run the **physical-port dither protect** command in global configuration mode. Frequently remove and insert the network cable on a physical port to simulate port flapping. Verify that a syslog indicating port flapping is displayed on the Console. After such a syslog is displayed for several times, the system prompts that the port will be shut down.

Configuration Example

Configuring Basic Attributes of Interfaces

Scenario **Figure 1-3**	
Configuration Steps	● Connect two devices through the switch ports. ● Configure an SVI respectively on two devices, and assign IP addresses from a network segment to the two SVIs. ● Enable interface index persistence on the two devices. ● Enable the link trap function on the two devices. ● Configure the interface administrative status on the two devices.
A	A# configure terminal A(config)# snmp-server if-index persist A(config)# interface vlan 1 A(config-if-VLAN 1)# ip address 192.168.1.1 255.255.255.0 A(config-if-VLAN 1)# exit A(config)# interface gigabitethernet 0/1 A(config-if-GigabitEthernet 0/1)# snmp trap link-status A(config-if-GigabitEthernet 0/1)# shutdown A(config-if-GigabitEthernet 0/1)# end A# write

B	B# configure terminal B(config)# snmp-server if-index persist B(config)# interface vlan 1 B(config-if-VLAN 1)# ip address 192.168.1.2 255.255.255.0 B(config-if-VLAN 1)# exit B(config)# interface gigabitethernet 0/1 B(config-if-GigabitEthernet 0/1)# snmp trap link-status B(config-if-GigabitEthernet 0/1)# shutdown B(config-if-GigabitEthernet 0/1)# end B# write
Verification	Perform verification on Switch A and Switch B as follows: ● Run the **shutdown** command on port GigabitEthern 0/1, and check whether GigabitEthern 0/1 and SVI 1 are Down. ● Run the **shutdown** command on port GigabitEthern 0/1, and check whether a trap indicating that this interface is Down is sent. ● Restart the device, and check whether the index of GigabitEthern 0/1 is the same as that before the restart.
A	A# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 **GigabitEthernet 0/1 is administratively down**, line protocol is DOWN Hardware is GigabitEthernet, address is 00d0.f865.de9b (bia 00d0.f865.de9b) Interface address is: no ip address MTU 1500 bytes, BW 1000000 Kbit Encapsulation protocol is Bridge, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Rxload is 1/255, Txload is 1/255 Queue Transmitted packets Transmitted bytes Dropped packets Dropped bytes 0 0 0 0 0 1 0 0 0 0 2 0 0 0 0 3 0 0 0 0 4 0 0 0 0 5 0 0 0 0 6 0 0 0 0 7 4 440 0 0 Switchport attributes: interface's description:"" lastchange time:0 Day:20 Hour:15 Minute:22 Second Priority is 0 admin medium-type is Copper, oper medium-type is Copper admin duplex mode is AUTO, oper duplex is Unknown admin speed is AUTO, oper speed is Unknown flow control admin status is OFF, flow control oper status is Unknown

	admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Port-type: access Vlan id: 1 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 0 bits/sec, 0 packets/sec 4 packets input, 408 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 4 packets output, 408 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets A# show interfaces vlan 1 Index(dec):4097 (hex):1001 VLAN 1 is UP, line protocol is DOWN Hardware is VLAN, address is 00d0.f822.33af (bia 00d0.f822.33af) **Interface address is: 192.168.1.1/24** ARP type: ARPA, ARP Timeout: 3600 seconds MTU 1500 bytes, BW 1000000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Rxload is 0/255, Txload is 0/255
B	B# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 **GigabitEthernet 0/1 is administratively down**, line protocol is DOWN Hardware is GigabitEthernet Interface address is: no ip address, address is 00d0.f865.de9b (bia 00d0.f865.de9b) MTU 1500 bytes, BW 1000000 Kbit Encapsulation protocol is Bridge, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Rxload is 1/255, Txload is 1/255 Queue Transmitted packets Transmitted bytes Dropped packets Dropped bytes 0 0 0 0 0 1 0 0 0 0 2 0 0 0 0 3 0 0 0 0 4 0 0 0 0 5 0 0 0 0 6 0 0 0 0 7 4 440 0 0 Switchport attributes: interface's description:"" lastchange time:0 Day:20 Hour:15 Minute:22 Second

```
    Priority is 0
    admin medium-type is Copper, oper medium-type is Copper
    admin duplex mode is AUTO, oper duplex is Unknown
    admin speed is AUTO, oper speed is Unknown
    flow control admin status is OFF, flow control oper status is Unknown
    admin negotiation mode is OFF, oper negotiation state is ON
    Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Port-type: access
    Vlan id: 1
   10 seconds input rate 0 bits/sec, 0 packets/sec
   10 seconds output rate 0 bits/sec, 0 packets/sec
    4 packets input, 408 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    4 packets output, 408 bytes, 0 underruns, 0 dropped
0 output errors, 0 collisions, 0 interface resets
B# show interfaces vlan 1
Index(dec):4097 (hex):1001
VLAN 1 is UP, line protocol is DOWN
Hardware is    VLAN, address is 00d0.f822.33af (bia 00d0.f822.33af)
Interface address is: 192.168.1.2/24
ARP type: ARPA, ARP Timeout: 3600 seconds
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec, set
  Carrier delay is 2 sec
  Rxload is 0/255, Txload is 0/255
```

1.4.2 Configuring Interface Attributes

Configuration Effect

- Enable the device to connect and communicate with other devices through the switch port or routed port.
- Adjust various interface attributes on the device.

Configuration Steps

Configuring the Medium Type of an Interface

- Optional.
- By default, the medium type of a combo port is copper.
- Port flapping may occur if the configured medium type of a port changes.
- This command is applicable to an Ethernet physical port or AP port.

Command	**medium-type** { **auto-select** [**prefer** [**fiber** | **copper**]] | **fiber** | **copper** }
Parameter Description	**auto-select**: Indicates that the medium type is selected automatically. **prefer** [**fiber** | **copper**]: Indicates the medium type that will be preferentially selected. **fiber**: Indicates that fiber is forcibly selected as the medium type.

	copper: Indicates that copper is forcibly selected as the medium type.
Defaults	By default, the medium type of an interface is copper.
Command Mode	Interface configuration mode
Usage Guide	Select either fiber or copper as the medium type of a port when both medium types are available. Once the medium type is selected, all interface attributes, including the status, duplex mode, and speed, are configured for the interface of the selected medium type. If the interface type is changed, the attributes of the new interface type are the default attributes. You can reconfigure these attributes as required. If you enable automatic selection of the medium type, the device uses the current medium if only one medium is available. If both media are available, the device uses the preferred medium as configured. By default, the preferred medium is copper. You can run the **medium-type auto-select prefer fiber** command to configure fiber as the preferred media. In automatic medium selection mode, the interface adopts the default settings of attributes, such as the speed, duplex mode, and flow control mode.

Configuring the Speed of an Interface

- Optional.
- Port flapping may occur if the configured speed of a port changes.
- This command is applicable to an Ethernet physical port or AP port.

Command	**speed** [**10** | **100** | **1000** | **auto**]
Parameter Description	**10**: Indicates that the speed of the interface is 10 Mbps. **100**: Indicates that the speed of the interface is 100 Mbps. **1000**: Indicates that the speed of the interface is 1000 Mbps. **auto**: Indicates that the speed of the interface automatically adapts to the actual condition.
Defaults	By default, the speed of an interface is auto.
Command Mode	Interface configuration mode
Usage Guide	If an interface is an AP member port, the speed of this interface is determined by the speed of the AP port. When the interface exits the AP port, it uses its own speed configuration. You can run **show interfaces** to display the speed configurations. The speed options available to an interface vary with the type of the interface. For example, you cannot set the speed of an SFP interface to 10 Mbps. The speed of a 40G physical port can only be set to 40 Gbps or auto.

Configuring the Duplex Mode of an Interface

- Optional.
- Port flapping may occur if the configured duplex mode of a port changes.
- This command is applicable to an Ethernet physical port or AP port.

Command	**duplex** { **auto** | **full** | **half** }
Parameter Description	**auto**: Indicates automatic switching between full duplex and half duplex. **full**: Indicates full duplex. **half**: Indicates half duplex.
Defaults	By default, the duplex mode of an interface is auto.
Command	Interface configuration mode

Mode	
Usage Guide	The duplex mode of an interface is related to the interface type. You can run **show interfaces** to display the configurations of the duplex mode.

Configuring the MTU of an Interface

- Optional.
- You can configure the MTU of a port to limit the length of a frame that can be received or sent over this port.
- This command is applicable to an Ethernet physical port or SVI.

Command	**mtu** *num*
Parameter Description	*num*: *64–9216*
Defaults	By default, the MTU of an interface is 1500 bytes.
Command Mode	Interface configuration mode
Usage Guide	This command is used to configure the interface MTU, that is, the maximum length of a data frame at the link layer. Currently, you can configure MTU for only a physical port or an AP port that contains one or more member ports.

Configuring the Bandwidth of an Interface

- Optional.
- Generally, the bandwidth of an interface is the same as the speed of the interface.

Command	**bandwidth** *kilobits*
Parameter Description	*kilobits*: The value ranges from 1 to 2,147,483,647. The unit is kilo bits.
Defaults	Generally, the bandwidth of an interface matches the type of the interface. For example, the default bandwidth of a gigabit Ethernet physical port is 1,000,000, and that of a 10G Ethernet physical port is 10,000,000.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the Carrier Delay of an Interface

- Optional.
- If the configured carrier delay is long, it takes a long time to change the protocol status when the physical status of an interface changes. If the carrier delay is set to 0, the protocol status changes immediately after the physical status of an interface changes.

Command	**carrier-delay {[milliseconds]** *num* **| up [milliseconds]** *num* **down [milliseconds]** *num***}**
Parameter Description	*num*: The value ranges from 0 to 60. The unit is second. *milliseconds*: Indicates the carrier delay. The value ranges from 0 to 60,000. The unit is millisecond. *Up*: Indicates the delay after which the state of the DCD changes from Down to Up. *Down*: Indicates the delay after which the state of the DCD changes from Up to Down.
Defaults	By default, the carrier delay of an interface is 2s.
Command Mode	Interface configuration mode
Usage Guide	If millisecond is used as the unit, the configured carrier delay must be an integer multiple of 100 milliseconds.

Configuring the Load Interval of an Interface

- Optional.

- The configured load interval affects computation of the average packet rate on an interface. If the configured load interval is short, the average packet rate can accurately reflect the changes of the real-time traffic.

Command	**load-interval** *seconds*
Parameter Description	*seconds*: The value ranges from 5 to 600. The unit is second.
Defaults	By default, the load interval of an interface is 10s.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring MAC Addresses for Interfaces

- Optional. If this function is required, run the **mac-address** command in interface configuration mode.
- By default, MAC addresses of interfaces have fixed values.

Command	**mac-address** *mac-address*
Parameter Description	***Mac-address***: Indicates a valid MAC address.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the VLAN Encapsulation Flag for Interfaces

- Optional. If this function is required, run the **encapsulation dot1Q** command in interface configuration mode.
- By default, the VLAN encapsulation protocol is disabled for interfaces.

Command	**encapsulation dot1Q** *VlanID*
Parameter Description	***VlanID***: Indicates the VLAN ID. The value range is from **1** to **4094**.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the Keepalive Packet Period for Interfaces

- Optional. If this function is required, run the **keepalive** command in interface configuration mode.
- By default, the keepalive function is disabled for Ethernet interfaces. For other WAN interfaces, the default keepalive packet period is 10s.

Command	**keepalive** [*keep-period* [*keep-retries*]]
Parameter Description	***keep-period***: Indicates the period for sending keepalive packets. The value range is from **1** to **32767**. ***keep-retries***: Indicates the maximum number of keepalive packet timeouts. The value range is from **1** to **255**.
Command Mode	Interface configuration mode
Usage Guide	N/A

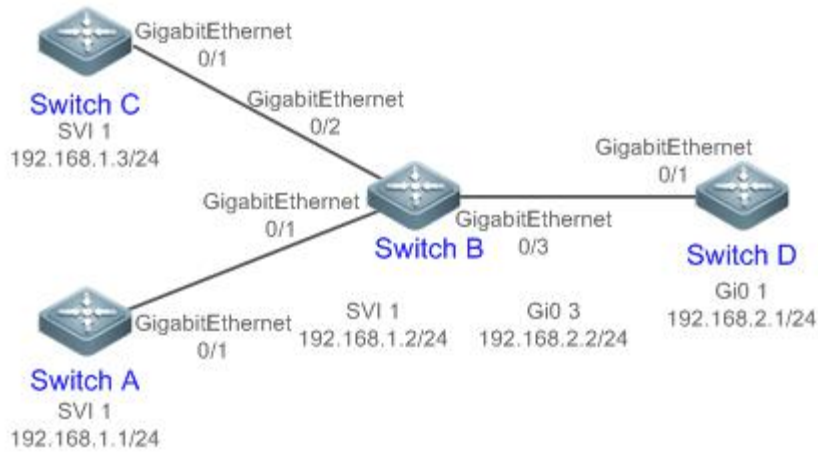
Verification

- Run the **show interfaces** command to display the attribute configurations of interfaces.

Command	**show interfaces** [*interface-type interface-number*] [**description**]

Configuration Example

Configuring Interface Attributes

Scenario Figure 1-4	
Configuration Steps	● On Switch A, configure GigabitEthernet 0/1 as an access mode, and the default VLAN ID is 1. Configure SVI 1, assign an IP address to SVI 1, and set up a route to Switch D. ● On Switch B, configure GigabitEthernet 0/1 and GigabitEthernet 0/2 as Trunk ports, and the default VLAN ID is 1. Configure SVI 1, and assign an IP address to SVI 1. Configure GigabitEthernet 0/3 as a routed port, and assign an IP address from another network segment to this port. ● On Switch C, configure GigabitEthernet 0/1 as an Access port, and the default VLAN ID is 1. Configure SVI 1, and assign an IP address to SVI 1. ● On Switch D, configure GigabitEthernet 0/1 as a routed port, assign an IP address to this port, and set up a route to Switch A.
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# switchport mode access A(config-if-GigabitEthernet 0/1)# switchport access vlan 1 A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip address 192.168.1.1 255.255.255.0 A(config-if-VLAN 1)# exit A(config)# ip route 192.168.2.0 255.255.255.0 VLAN 1 192.168.1.2
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# switchport mode trunk B(config-if-GigabitEthernet 0/1)# exit B(config)# interface GigabitEthernet 0/2 B(config-if-GigabitEthernet 0/2)# switchport mode trunk B(config-if-GigabitEthernet 0/2)# exit B(config)# interface vlan 1 B(config-if-VLAN 1)# ip address 192.168.1.2 255.255.255.0 B(config-if-VLAN 1)# exit B(config)# interface GigabitEthernet 0/3 B(config-if-GigabitEthernet 0/3)# no switchport

	B(config-if-GigabitEthernet 0/3)# ip address 192.168.2.2 255.255.255.0 B(config-if-GigabitEthernet 0/3)# exit
C	C# configure terminal C(config)# interface GigabitEthernet 0/1 C(config-if-GigabitEthernet 0/1)# port-group 1 C(config-if-GigabitEthernet 0/1)# exit C(config)# interface aggregateport 1 C(config-if-AggregatePort 1)# switchport mode access C(config-if-AggregatePort 1)# switchport access vlan 1 C(config-if-AggregatePort 1)# exit C(config)# interface vlan 1 C(config-if-VLAN 1)# ip address 192.168.1.3 255.255.255.0 C(config-if-VLAN 1)# exit
D	D# configure terminal D(config)# interface GigabitEthernet 0/1 D(config-if-GigabitEthernet 0/1)# no switchport D(config-if-GigabitEthernet 0/1)# ip address 192.168.2.1 255.255.255.0 D(config-if-GigabitEthernet 0/1)# exit A(config)# ip route 192.168.1.0 255.255.255.0 GigabitEthernet 0/1 192.168.2.2
Verification	Perform verification on Switch A, Switch B, Switch C, and Switch D as follows: ● On Switch A, ping the IP addresses of interfaces of the other three switches. Verify that you can access the other three switches on Switch A.. ● Verify that switch B and Switch D can be pinged mutually. ● Verify that the interface status is correct.
A	A# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is UP, line protocol is UP Hardware is GigabitEthernet, address is 00d0.f865.de90 (bia 00d0.f865.de90) Interface address is: no ip address MTU 1500 bytes, BW 100000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Admin medium-type is Copper, oper medium-type is Copper Admin duplex mode is AUTO, oper duplex is Full Admin speed is AUTO, oper speed is 100M Flow control admin status is OFF, flow control oper status is OFF Admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF

	Rxload is 1/255, Txload is 1/255 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 67 bits/sec, 0 packets/sec 362 packets input, 87760 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 363 packets output, 82260 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets
B	B# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is UP, line protocol is UP Hardware is GigabitEthernet, address is 00d0.f865.de91 (bia 00d0.f865.de91) Interface address is: no ip address MTU 1500 bytes, BW 100000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Admin medium-type is Copper, oper medium-type is Copper Admin duplex mode is AUTO, oper duplex is Full Admin speed is AUTO, oper speed is 100M Flow control admin status is OFF, flow control oper status is OFF Admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Bridge attributes: Rxload is 1/255, Txload is 1/255 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 67 bits/sec, 0 packets/sec 362 packets input, 87760 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 363 packets output, 82260 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets
C	C# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is UP, line protocol is UP Hardware is GigabitEthernet, address is 00d0.f865.de92 (bia 00d0.f865.de92) Interface address is: no ip address MTU 1500 bytes, BW 100000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set

	Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Admin medium-type is Copper, oper medium-type is Copper Admin duplex mode is AUTO, oper duplex is Full Admin speed is AUTO, oper speed is 100M Flow control admin status is OFF, flow control oper status is OFF Admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Rxload is 1/255, Txload is 1/255 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 67 bits/sec, 0 packets/sec 362 packets input, 87760 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 363 packets output, 82260 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets
D	D# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is UP, line protocol is UP Hardware is GigabitEthernet, address is 00d0.f865.de93 (bia 00d0.f865.de93) **Interface address is: 192.168.2.1/24** MTU 1500 bytes, BW 100000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Admin medium-type is Copper, oper medium-type is Copper Admin duplex mode is AUTO, oper duplex is Full Admin speed is AUTO, oper speed is 100M Flow control admin status is OFF, flow control oper status is OFF Admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Rxload is 1/255, Txload is 1/255 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 67 bits/sec, 0 packets/sec 362 packets input, 87760 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort

	363 packets output, 82260 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets

1.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears the counters of a specified interface.	**clear counters** [*interface-type interface-number*]
Resets the interface hardware.	**clear interface** *interface-type interface-number*

Displaying

Displaying Interface Configurations and Status

Description	Command
Displays all the status and configuration information of a specified interface.	**show interfaces** [*interface-type interface-number*]
Displays the interface status.	**show interfaces** [*interface-type interface-number*] **status**
Displays the interface errdisable status.	**show interfaces** [*interface-type interface-number*] **status err-disable**
Displays the link status change time and count of a specified port.	**show interfaces** [*interface-type interface-number*] **link-state-change statistics**
Displays the description and status of a specified interface.	**show interfaces** [*interface-type interface-number*] **description**
Displays the bandwidth usage of an interface.	**show interfaces** [*interface-type interface-number*] **usage**

2 Configuring MODE-MGMT

2.1 Overview

With mode management, you can achieve unified management on system mode, internal and external network attributes of network interfaces, and so on.

FS gateway products can serve as both gateways (gateway mode) and bridges (bridge mode). These two modes can be switched through mode management.

In bridge mode, the gateway products support four operating modes: forward mode, sniffer mode, software bypass mode, and one-arm mode. Users can configure the operating mode based on their requirements.

When the device is connected to the network, you will have an internal network and an external network. Consequently, the device's interfaces also have internal and external network attributes. Mode management enables you to switch between internal and external network attributes for interfaces, to facilitate your adjustment based on actual situation.

Protocols and Standards

- N/A

2.2 Applications

Application	Description
Switching Internal and External Network Attributes of Interfaces	The user network topology changes or an external line is added.
Switching Bridge Operating Mode	Changes the operating mode of the bridge.

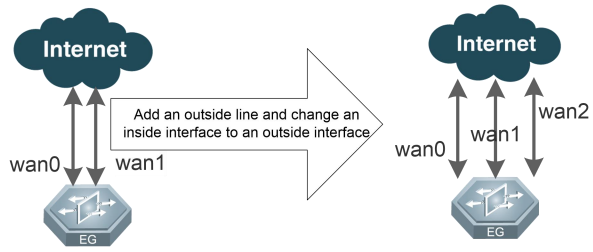
2.2.1 Switching Internal and External Network Attributes of Interfaces

Scenario

It is required to connect an outside interface when user network topology changes, for example, when an external line is added.

In the case that all outside interfaces are occupied while some inside interfaces are still idle, you can change inside interfaces to outside interfaces to support line expansion.

Figure 2- 1



Remarks	In this example, the device has two outside interfaces wan1 and wan0; the rest are inside interfaces. When an external line is added, change an idle inside interface to an outside interface, that is, wan2.

Deployment

- Determine the idle inside interface to be switched.
- Execute the switching command to configure the interface as an outside interface.

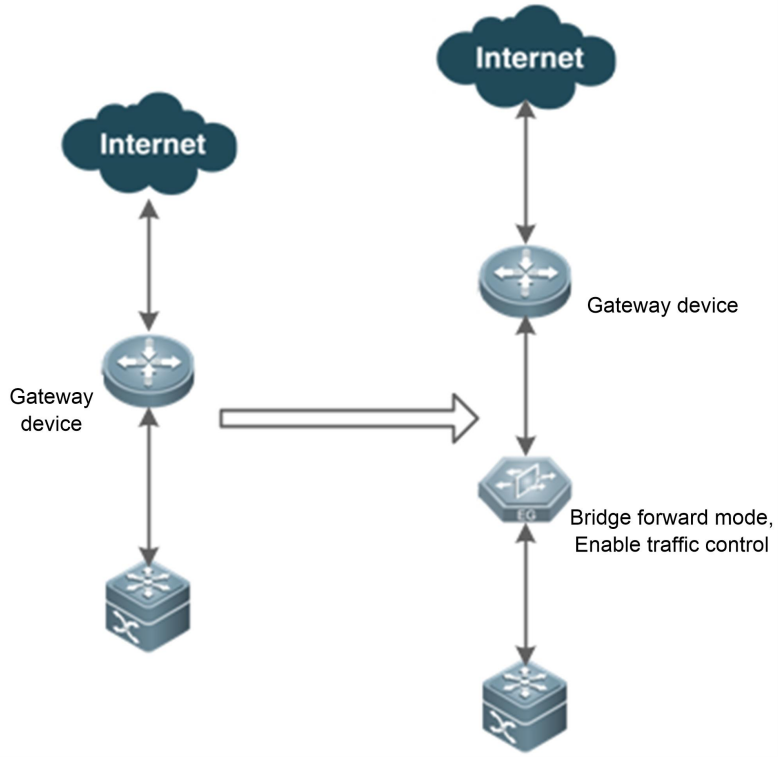
- Save the configuration and reboot the device to validate the configuration.

2.2.2 Switching Bridge Operating Mode

Scenario

You can switch the system mode between gateway and bridge depending on specific applications of the device. If you want to use it as a bridge, you need to switch it to the bridge mode and specify the bridge operating mode. In bridge mode, the device supports four operating modes (the MSC supports five operating modes), each for different purposes. You can switch between these operating modes based on actual needs.

Figure 2- 2



Remarks	In this example, you have a gateway device originally. Later you have needs for traffic control while keeping the original gateway device. Then you can switch the gateway device to the bridge mode, connect it to the current network, and configure it as forward mode. It then provides traffic identification and traffic control functions.

Deployment

- Determine the current system mode. If it is not a bridge, switch it to the non-gateway mode using the switching command, save the configuration and reboot the device.
- Choose an inside interface and an outside interface to establish a bridge-map; configure its operating mode and connect it to the network.
- If you need more bridges, repeat the previous step.
- If you need to change the bridge operating mode, enter the bridge configuration mode and make modifications.

2.3 Features

Basic Concepts

System Mode

There are two system modes: gateway mode and bridge mode (non-gateway mode). Some of the devices support both system modes.
When the device operates in gateway mode, all interfaces are layer 3 ones and packets are forwarded according to the routing table. Packet processing in gateway mode resembles that on a common router, so no further description is given here.
When the device operates in bridge mode, all interfaces are layer 2 ones and packets are forwarded according to the bridge-map. In this mode, no modification is made for normally forwarded packets, except that packets may be blocked or discarded due to particular traffic polices.
The default mode is bridge mode.
The device cannot operate in both the gateway and bridge modes.
When switching from gateway to bridge, or from bridge to gateway, you need to save the configuration and reboot the device to validate the configuration.

Internal and External Network Attributes

For the gateway products, all interfaces except the MGMT interface (management interface) have internal or external network attributes. You need to configure internal and external network attributes for interfaces according to the actual situation: inside interfaces connect the intranet, while outside interfaces connect the external line.
You can query information about mode management to learn the internal and external network attributes for each interface. Using the configuration command, you can modify the internal or external network attributes of interfaces.
Here interfaces refer to the physical ports on the device. Accordingly, their sub-interfaces will inherit their internal and external network attributes, and vary with the attributes of these physical ports; some virtual interfaces on the device, such as the dialer interface, only have external network attributes, and do not support attributes switching.
When switching internal and external network attributes of interfaces, you need to save the configuration and reboot the device to validate the configuration.

Bridge Operating Mode

In bridge mode, packets are forwarded according to the bridge-map. No modification is made for normally forwarded packets, except that packets may be blocked or discarded due to particular traffic polices.
Each bridge-map needs to be associated with an inside interface and an outside interface, and the operating mode for the non-gateway mode should be specified. The bridge mode supports these operating modes:

- Forward: Traffic identification, traffic blocking, traffic control and traffic auditing can be performed for packets passing the device.
- Sniffer: Traffic identification and traffic auditing can be performed for packets passing the device.
- Bypass: Traffic statistics are gathered at interfaces for packets passing the device.
- Receive-only: Also known as the one-armed mode. Traffic identification and traffic auditing can be performed for packets passing the device. The only difference is that packets are discarded after processing, instead of being forwarded.

The number of bridge-maps depends on the maximum number of inside-outside interface pairs that the device can provide. For example, if the device has four inside interfaces and four outside interfaces, you can define up to four bridge-maps. If the device has four inside interfaces and three outside interfaces, you can configure only 3 bridge-maps. Different devices may support different number of bridge-maps.

Bridge-maps cannot be removed; they become valid when the operating mode is defined.

If the system has multiple bridge-maps, you can configure different operating modes for different bridge-maps.

Overview

Feature	Description
Configuring System Mode	Configures the device operating in non-gateway mode or gateway mode.

Configuring Internal and External Network Attributes	Configures the internal and external network attributes of interfaces according to the actual network topology.
Configuring Bridge Operating Mode	Configures the operating mode of a pair of bridges. Different operating modes support different traffic processing modes.
Configuring Hardware Bypass	Configures hardware bypass when the device operates abnormally, so as to prevent network link interruption.
Configuring Switching Between Layer-2 and Layer-3 Ports	Switches a layer-2 port into a layer-3 port, or vice versa.
Configuring Port VLAN of a Layer-2 Port	Adds some layer-2 ports to a VLAN and specifies whether the VLAN is tagged.
Configuring Native VLAN of a Layer-2 Port	Configures a native VLAN on a layer-2 port.
Configuring Layer-2 Port Mirroring	Configures a layer-2 port to monitor the packets of the other layer-2 ports.

2.3.1 Configuring System Mode

Configure the device operating in non-gateway mode or gateway mode.

Working Principle

In different system modes, the system supports different services. The biggest difference is that the device in gateway mode supports layer-3 routing, while the device in bridge mode provides only layer-2 forwarding. According to your needs, you can switch between the gateway and bridge modes.

Related Configuration

Configuring System Mode

The MSC devices operate in bridge mode by default. The ACE devices only support the bridge mode. The NBR devices only support the gateway mode.

EG devices operate in bridge mode by default. You can use the **sys-mode gateway** command to switch the system mode. Save the configuration and reboot the device to validate the configuration.

2.3.2 Configuring Internal and External Network Attributes

Configure the internal and external network attributes of interfaces according to the actual network topology.

Working Principle

Inside and outside interfaces process different transactions. For example, traffic auditing and traffic control are based on outside interfaces. Improper configuration may affect normal transaction processing on the interface. Internal and external network attributes are of software nature. You can modify them according to the actual network topology, and related transactions will be adjusted accordingly.

Related Configuration

Configuring Internal and External Network Attributes

By default, different interfaces on the device have different internal and external network attributes and they are configured based on the most typical user scenarios. You can display specific attributes on the Web management page or in the configuration file.

You can use the **specify interface** *interface-name* **{ lan | wan }** command to switch the internal and external network attributes of an interface. Save the configuration and reboot the device to validate the configuration.

2.3.3 Configuring Bridge Operating Mode

Configure the operating mode of a pair of bridges. Different operating modes support different traffic processing modes.

Working Principle

In forward, sniffer and bypass mode of the bridge mode, packet forwarding is based on the bridge-map. Packets that enter from the inside interface of the bridge-map are forwarded out of the paired outside interface; packets that enter from the outside interface are forwarded out of the paired outside interface. In one-armed mode, packets are discarded instead of being forwarded. Of course, in one-armed mode, you need to configure the IP address segment of the internal network to determine whether packets are in the uplink or downlink direction.

Related Configuration

- **Entering bridge-map Configuration Mode**

You can use the **bridge-map** *bridge-num* command to create a bridge-map and enter the bridge-map configuration mode.

- **Configuring bridge-map Operating Mode**

No operating mode is configured for the bridge-map by default.

You can use the **link-mode** *interface-name1 interface-name2* **{ forward | sniffer | bypass | receive-only }** command to configure a bridge-map and specify its operating mode.

You can use the **lan-ip** *ip_address subnet_mask* command to configure the IP address segment of the internal network in one-armed mode. A one-armed mode supports up to 100 IP address segments of the internal network.

2.3.4 Configuring Hardware Bypass

Configure hardware bypass when the device operates abnormally, so as to prevent network link interruption.

Working Principle

The hardware bypass function implements interconnection between two network interfaces via a hardware circuit. When the bypass function is enabled, a network cable is inserted into the two interfaces and the interfaces are in the down state. This makes the two interfaces and the cable equivalent to one cable; but the two ends of the device are connected. Packets are not sent to the software of the device.

Related Configuration

- **Configuring Hardware Bypass**

The hardware bypass function of the device is disabled by default.

Use the **bypass** command to enable the hardware electrical port bypass function.

2.3.5 Configuring Function of Not Storing Logs in Local Hard Disk

Enable the function of not storing logs in local hard disk. Information such as device audit logs, traffic audit logs, content audit logs, and flow logs are not recorded in the hard disk.

Working Principle

When the number of users on one device exceeds a certain value (10,000 for EG2000X/XE/UE and ACE3000E; 5000 for EG2000G/GE and ACE2000E; other products do not support this function), a large amount of information is stored in the local hard disk, which affects the performance of the device. In this case, it is recommended to enable the function of not storing logs in local hard disk. When this function

is enabled, relevant log information such as device audit logs, traffic audit logs, content audit logs, and flow logs are not stored in the local hard disk but will be sent to an external server through the log service of the device.

Related Configuration

Configuring Function of Not Storing Logs in Local Hard Disk

The function of not storing logs in local hard disk is enabled by default for EG2000X/XE/UE and ACE3000E and is disabled by default for EG2000G/GE and ACE2000E. Other gateway products do not support this function.

Use the **write-db enable** command to disable this function, and use the ***no** form of this command to enable this function: **no write-db enable**.

2.3.6 Configuring Switching Between Layer-2 and Layer-3 Ports

Some products have both layer-2 ports and layer-3 ports. A layer-3 port can be used to connect an egress line, while a layer-2 port can be used to connect an intranet. In actual application, multiple egress lines or more layer-3 ports are needed for connection to other devices, and the number of layer-3 ports needed may exceed the number of fixed ports that the device can provide. In this situation, use this function to switch the specified layer-2 port into a layer-3 port, or switch the layer-3 port back to the layer-2 port, to dynamically meet various user requirements.

Working Principle

A layer-3 port is an independent port for users. If a layer-2 port is switched into a layer-3 port, it is the same as a fixed layer-3 port. If this layer-3 port is switched back to the layer-2 port, all the previous configuration on this layer-3 port will be invalidated.

Related Configuration

Configuring Layer-2 and Layer-3 Switching

This function is supported only on the first five ports on the panel of EG2000K and EG2000L and only on the first three ports on the panel of NBR1300G-E. All the ports are layer-2 ports by default.

Use the **convert** command to change the layer-2/layer-3 attribute of a port and specify the initial internal/external network attribute of a layer-3 port.

2.3.7 Configuring Port VLAN of a Layer-2 Port

The port VLAN function allows adding one or more layer-2 ports to the same VLAN with an 802.1Q tag. Only these ports can receive the packets with the 802.1Q VLAN tag and these packets are not sent to other ports that do not belong to this VLAN, so as to implement port isolation. This configuration is usually used in LAN planning. To ensure security, the LAN is divided into multiple small logical networks through VLAN configuration to implement network isolation.

Working Principle

Implement flexible division and management of a LAN by setting VLANs on a layer-2 port.

Related Configuration

Configuring VLAN of a Layer-2 Port

Only the layer-2 ports of EG2000K, EG2000L, and NBR1300G-E support the port VLAN function.

All layer-2 ports are located in VLAN 4089 by default.

Run the **vlan port** command to add some ports into a VLAN.

2.3.8 Configuring Native VLAN of a Layer-2 Port

A default VLAN tag will be automatically added to packets that are sent and received by a port in a native VLAN and do not carry a VLAN tag. This default VLAN tag is the ID of the native VLAN.

Generally, all layer-2 ports (also called "ports") of a device belong to a system-preset native VLAN. These ports can exchange and forward packets. As a result, flooding and security issues may occur on the ports. In this case, the native VLAN of each port can be changed to implement port isolation.

Working Principle

All ports of a device are located in a system-preset native VLAN and are in the same broadcast domain. When the native VLAN of a port is changed to another native VLAN, this port is removed from the preset native VLAN to implement port isolation.

Packets that are received through a port and carry a native VLAN tag or do not carry a VLAN tag will be untagged when being forwarded.

Related Configuration

Configuring Native VLAN of a Layer-2 Port

Only the layer-2 ports of EG2000K, EG2000L, and NBR1300G-E support the native VLAN function.

All layer-2 ports are located in Native VLAN 4089 by default.

Use the **native** command to change the native VLAN of a layer-2 port.

2.3.9 Configuring Layer-2 Port Mirroring

The layer-2 port mirroring is a monitoring method provided for the network administrator and can duplicate traffic of one port to another for sending. It allows the network administrator to analyze port traffic in real time.

Working Principle

A port must be selected as a monitoring port to implement the port monitoring function. One or more other ports can be added to the monitoring list of the monitoring port, and the monitoring direction (receiving direction, sending direction, and receiving and sending direction) can be configured separately for each port as required. The monitored ports will duplicate sent/received packets to the monitoring port. Generally the monitoring port is connected to the PC and captures and analyzes the packets by packet capture software.

Related Configuration

Configuring Layer-2 Port Mirroring

Only the layer-2 ports of EG2000K, EG2000L, and NBR1300G-E support the port mirroring function.

The port mirroring function is disabled by default.

Use the **mirror** command to enable the mirroring function.

2.4 Limitations

EG2000CE does not support 10GE ports; EGEG3000XE and EG3000UE support 10GE ports.

EGEG3000XE and EG3000UE have eight fixed 10GE ports in total.

EG3000XE and EG3000UE support NPE mode; EG2000CE does not support NPE mode. By default, the mode is enabled on EG3000XE and EG3000UE.

2.5 Configuration

Configuration	Description and Command

Configuring System Mode	(Optional) It is used to switch the system mode between gateway and bridge. The EG serves in gateway mode by default.	
	sys-mode gateway	Sets the system mode to gateway
	no sys-mode gateway	Sets the system mode to bridge
Configuring Internal and External Network Attributes	(Optional) Defaults have been set. It is used to switch the internal and external network attributes of the interface.	
	specify interface *interface-name* { **lan** / **wan** }	Configures the internal and external network attributes of the interface
Configuring Bridge Operating Mode	(Mandatory) It is used to configure the bridge-map and its operating mode.	
	bridge-map *bridge-num*	Enters the bridge-map command mode layer
	link-mode *interface-name1 interface-name2* { **forward** | **sniffer** | **bypass** | **receive-only** }	Configures the bridge-map and operating mode for inside and outside interfaces.
	(Optional) The native-VLAN ID is 1 by default. It is used for category identification. Packets without VLAN tag are classified as VLAN objects corresponding to the currently configured VLAN ID.	
	native-vlan *vlan-id*	Configures the native-VLAN ID value of the bridge-map. Packets without vlan tag are identified as VLAN classification objects corresponding to the currently configured VLAN ID.
Configuring Hardware Bypass	(Optional) It is used to enable or disable the hardware bypass function. The hardware bypass function is disabled by default.	
	bypass couple *couple-num*	Enables a specified hardware bypass pair.
Configuring Switching Between GE and 10GE Ports	(Optional) It is used to switch between four GE ports and one 10GE port.	
	xaui-mode slot *slot-num*	Switches four GE ports into one 10GE port. *slot-num*: Indicates the slot ID of the 10GE port to be switched.
Configuring Function of Not Storing Logs in Local Hard Disk	(Optional) It is used to enable/disable the function of not storing logs in local hard disk. The default settings of different devices vary.	
	no write-db enable	Enables the function of not storing logs in local hard disk.
	write-db enable	Disables the function of not storing logs in local hard disk.
Configuring Switching Between Layer-2 and Layer-3 Ports	(Optional) It is used to switch between the layer-2 and layer-3 attributes of a port.	
	convert port *num* **to** { **wan** | **lan** }	Switches a layer-2 port into a layer-3 port and specifies the internal and external network attributes.
	no convert port *num*	Switches a layer-3 port into a layer-2 port.
Configuring Port VLAN of a Layer-2 Port	(Optional) It is used to configure the VLAN to which a layer-2 port belongs.	
	vlan port *min max* [**tag**]	Adds all layer-2 ports in the range of [min, max] to a VLAN and specifies whether a tag is carried.
	no vlan port	Removes all layer-2 ports from a VLAN.
Configuring Native VLAN of a	(Optional) It is used to configure the native VLAN of a port.	

Layer-2 Port	**native lan** *num* **vid** *vlan-id*	Configures the native VLAN of a port.
	no native lan *num*	Restores the default native VLAN (4089) of a port.
Configuring Layer-2 Port Mirroring	(Optional) It is used to configure a layer-2 port mirroring rule.	
	mirror master port *master_port* **slave port** *slave_port* **{ rx | tx | all }**	Sets port mirroring.
	no mirror master port *master_port* **slave port** *slave_port* **{ rx | tx | all }**	Deletes port mirroring.
Configuring Switching Between 40GE and 10GE Ports	(Optional) It is used to switch between one 40GE port and four 10GE ports.	
	split slot *slot-num*	Splits one 40GE port into four 10GE ports. *slot-num*: Specifies the slot ID of the 40GE port to be split.

2.5.1 Configuring System Mode

Configuration Effect

- Switch the system mode between gateway and bridge.

Notes

- Save the configuration and reboot the device to validate the configuration.

Configuration Steps

Configuring System Mode

- Optional
- An EG device serves in gateway mode by default.
- Configure it in global configuration mode.

Verification

You can use the **show sys-mode** command to display the current system mode.

Related Commands

Configuring System Mode

Command	**[no] sys-mode gateway**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Save the configuration and reboot the device to validate the configuration.

Displaying Current System Mode

Command	**show sys-mode**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Examples

Configuring System Mode to Bridge

Configuration Steps	• Switch the system mode to bridge. • Save the configuration and reboot the device.

	FS# configure terminal FS(config)# no sys-mode gateway FS(config)# exit FS#write Building configuration... [OK] FS#reload Reload system?(Y/N)y …
Verification	When the device is rebooted, use the **show sys-mode** command to verify whether the configuration is successful. ● Display the current system mode.
	FS# show sys-mode System is bridge mode. … LAN: GigabitEthernet 0/0 GigabitEthernet 0/3 GigabitEthernet 0/5 WAN: GigabitEthernet 0/1 GigabitEthernet 0/2 GigabitEthernet 0/4

Common Errors

- After switching the system mode, you reboot the device without saving the configuration or do not reboot the device after saving the configuration.

2.5.2 Configuring Internal and External Network Attributes

Configuration Effect

- Configure internal and external network attributes of interfaces based on the actual network topology.
- Usually, you need to make such adjustment when the device is powered on or when the network line changes.

Notes

- N/A

Configuration Steps

- Switch internal and external network attributes with the command.

Verification

- You can use the system mode query command to display the current internal and external network attributes.

Related Commands

Configuring Internal and External Network Attributes

Command	**specify interface** *interface-name* { **lan** / **wan** }
Parameter Description	**interface** *interface-name*: Interface name to be specified.
Command Mode	Global configuration mode

Usage Guide	Use the **no** form of this command to restore the original internal and external network attributes of the current interface.

Displaying Internal and External Network Attributes of All Interfaces

Command	**show sys-mode**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Examples

Adding a New External Line (All Three Outside Interfaces Are Occupied and Some Inside Interfaces Are Still Idle. You Switch an Idle Inside Interface to an Outside Interface.)

Configuration Steps	● Switch an idle inside interface to an outside interface.
	FS# configure terminal FS(config)# specify interface GigabitEthernet 0/3 wan FS(config)# end
Verification	● Use the show command to display the configuration results.
	FS# show sys-mode System is bridge mode. … LAN: GigabitEthernet 0/0 GigabitEthernet 0/5 WAN: GigabitEthernet 0/1 GigabitEthernet 0/2 GigabitEthernet 0/3 GigabitEthernet 0/4

Common Errors

- N/A

2.5.3 Configuring Bridge Operating Mode

Configuration Effect

- You can the bridge operating mode as needed. Different services are provided in different operating modes.

Notes

- A bridge-map must comprise an inside interface and an outside interface. One interface cannot belong to several bridge-maps.
- You must define an operating mode for the bridge-map to make the bridge operate normally.

Configuration Steps

- Enter the bridge-map mode configuration layer
- In bridge mode, no defaults are set for the bridge-map. Configure an inside interface and an outside interface to comprise a bridge-map and define its operating mode to any one of the forward, sniffer, bypass and one-armed modes.

Verification

- Use the bridge operating mode query command to verify the results.

Related Commands

Entering bridge-map Mode Configuration Layer

Command	**bridge-map** *bridge-num*
Parameter Description	*bridge-num*: Bridge-map No.
Command Mode	Global configuration mode
Usage Guide	N/A

Specifying Internal and External Interfaces and Bridge Operating Mode

Command	**link-mode** *interface-name1 interface-name2* { **forward | sniffer | bypass | receive-only** }
Parameter Description	*interface-name1*: Name of the internal interface. *interface-name2*: Name of the external interface.
Command Mode	bridge-map configuration mode
Usage Guide	N/A

Defining Native-VLAN ID

Command	**native-vlan** *vlan-id*
Parameter Description	*vlan-id*: Native-VLAN ID of the bridge-map.
Command Mode	bridge-map configuration mode
Usage Guide	Packets without vlan tag are classified as VLAN objects corresponding to the currently configured VLAN ID.

Displaying Internal and External Network Attributes of All Interface

Command	**show bridge-map** [*bridge-num*] [**lan-ip**]
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Examples

Using the Device as a Bridge and Attempting to Carry Out Traffic Control for Packets Passing It (You Configure the Device Operating in Forward Mode.)

Configuration Steps	● Enter the bridge-map configuration layer. ● Create a bridge-map and set its operating mode to forward.
	FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# bridge-map *0* FS(config-bridge-map)# link-mode *GigabitEthernet 0/0 GigabitEthernet 0/1* forward FS(config-bridge-map))# end
Verification	● You can use the **show bridge-map** command to display the results.
	FS#show bridge-map 0 BRIDGE MAP 0,STATE is DOWN Inside interface is GigabitEthernet 0/0,Outside interface is GigabitEthernet 0/1 Working mode is forward Native vlan is 1

Using the Device as a Bypass Device and Setting Its Operating Mode to One-armed to Audit Packets Mirrored from the Switch

Configuration Steps	● Enter the bridge-map configuration layer. ● Create a bridge-map and set its operating mode to one-armed (receive-only). ● Configure the IP address segment of the inside network.
	FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# bridge-map *0* FS(config-bridge-map)# link-mode *GigabitEthernet 0/0 GigabitEthernet 0/1* receive-only FS(config-bridge-map)# lan-ip *192.168.0.0 255.255.255.0* FS(config-bridge-map)# lan-ip *10.10.10.0 255.255.255.0* FS(config-bridge-map))# end
Verification	● You can use the **show bridge-map** command to display the results.
	FS#show bridge-map 0 BRIDGE MAP 0,STATE is DOWN Inside interface is GigabitEthernet 0/0,Outside interface is GigabitEthernet 0/1 Working mode is receive-only Native vlan is 1 FS#show bridge-map 0 lan-ip IP add mask add 192.168.0.0 255.255.255.0 10.10.10.0 255.255.255.0

Common Errors

● The bridge configuration does not meet actual needs. For example, you want to carry out traffic control, but do not configure the device's operating mode as forward.

● A bridge-map consists of an inside interface and an outside interface. Two interfaces with the same internal or external network attributes cannot be configured to form a bridge-map.

2.5.4 Configuring Hardware Bypass

Configuration Effect

● Enable or disable the hardware bypass function.

Notes

● In general, the hardware bypass function does not need to be enabled.

Configuration Steps

● Run the **hardware Bypass** command to configure hardware bypass.

Verification

● Use the mode display command to display the current hardware bypass information.

Related Commands

↘ **Configuring Hardware Bypass**

Command	**bypass couple** *couple-num*

Parameter Description	*couple-num:* Specifies a hardware bypass pair to be enabled.
Command Mode	Global configuration mode
Usage Guide	Run the ***no** form of this command to disable a hardware bypass pair.

Displaying Current Hardware Bypass Status

Command	**show running-config**
Parameter Description	**N/A**
Command Mode	Privileged EXEC Mode
Usage Guide	N/A

Configuration Example

Enabling Hardware Bypass Pair

Configuration Steps	● Configure the first hardware electrical port bypass pair (numbered 0) of a device.
	FS(config)#bypass couple 0 Couple 0 bypass started.
Verification	● Run the **show** command to display the configuration result.
	FS#show running-config … bypass couple 0 …

2.5.5 Configuring Switching Between GE and 10GE Ports

Configuration Effect

- Switch between four GE ports and one 10GE port.

Notes

- The configuration can take effect only after the device is restarted.

Configuration Steps

- Run the **xaui-mode** command in global configuration mode to configure the switching.

Verification

- Display the port information after the device is restarted.

Related Commands

Configuring 10GE Port Mode

Command	**xaui-mode slot** *slot-num*
Parameter Description	*slot-num*: Indicates the slot ID of the 10GE port to be switched.
Command	Global configuration mode

Mode	
Usage Guide	Run the ***no** form of this command to disable the 10GE port mode.

Displaying Current 10GE Port Mode

Command	**show interface**
Parameter Description	**N/A**
Command Mode	Privileged EXEC Mode
Usage Guide	N/A

Configuration Example

Switching the First Four GE Ports to One 10GE Port

Configuration Steps	● Switch the first four GE ports into one 10GE port.
	FS(config)#xaui-mode slot 2 Please save the config, and reload system to take effect!
Verification	● After the device is restarted, run the **show** command to display the configuration result.
	FS#show interface … ========== TenGigabitEthernet 0/2 ========== …

2.5.6 Configuring Switching Between Layer-2 and Layer-3 Ports

Configuration Effect

- Configure switching between a layer-2 port and a layer-3 port and specify the initial internal and external network attributes.

Notes

- Port 0 cannot be switched.
- The command is valid only after the configuration is saved and the device is restarted.

Configuration Steps

- Run the **convert** command to configure switching between layer-2 and layer-3 ports.

Verification

- Before restarting the device, run the **show switch-info** command to display the configuration status.
- After restarting the device, display the information about created interfaces.

Related Commands

Switching Layer-2 Port into Layer-3 Port and Specifying Initial Internal and External Network Attributes

Command	**convert port** *num* **to { wan | lan }**
Parameter Description	*num*: Indicates the port ID. The range is from 1 to 4.
Command Mode	Global configuration mode

Usage Guide	Run the **no convert port** *num* command to switch a layer-3 port into a layer-2 port.

Displaying Current Layer-2 and Layer-3 Attributes

Command	**show switch-info**
Parameter Description	**N/A**
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	N/A

Configuration Example

Switching Port 2 into Layer-3 LAN Port and Switching Port 4 into Layer-3 WAN Port

Configuration Steps	
	FS(config)#convert port 2 to lan ##### Please save config and reload the system!!!!! FS(config)#convert port 4 to wan ##### Please save config and reload the system!!!!! FS(config)#
Verification	● Run the **show** command to display the configuration result.
	PORT0 LAN6 0 PORT1 PORT1 1 PORT2 LAN4 1 PORT3 PORT3 1 PORT4 WAN2 1

Common Errors

- A layer-3 port cannot be switched into a layer-3 port.

2.5.7 Configuring Port VLAN of a Layer-2 Port

Configuration Effect

- Configure a VLAN of a layer-2 port.

Notes

- All layer-2 ports are located in VLAN 4089 by default.
- The 802.1Q VLAN must be configured on a sub interface before configuring a port VLAN of a layer-2 port.
- This command takes effect only to layer-2 ports, regardless of whether a layer-3 port exists the port range.

Configuration Steps

- Run the **vlan port** command to configure a port VLAN of a layer-2 port.

Verification

- Run the **show running-config** command to display the current configuration status.

Related Commands

Configuring VLAN of Layer-2 Port

Command	**vlan port** *min max* **[tag]**
Parameter Description	*min/max*: Specifies the port range in the format of [min, max]. The parameter value is **[0, 4]**, and the value of **max** is greater than or equal to that of **min**. *tag*: Specifies whether the VLAN is tagged.
Command Mode	Sub interface mode
Usage Guide	Run the **no vlan port** command to remove all ports from the VLAN.

Displaying the Configuration

Command	**show running-config**
Parameter Description	**N/A**
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	N/A

Configuration Example

Adding Port 1 and Port 2 to VLAN 100 without a Tag.

Configuration Steps	● Add Port 1 and Port 2 to VLAN 100 without tagging their packets..
	FS(config-subif-GigabitEthernet 0/0.1)#encapsulation do FS(config-subif-GigabitEthernet 0/0.1)#encapsulation dot1Q 100 *Oct 23 11:10:27: %7: Command is OK! *Oct 23 11:10:27: %7: Notice: please use command 'vlan port' to add vlan entry. FS(config-subif-GigabitEthernet 0/0.1)#vlan port 1 2 FS(config-subif-GigabitEthernet 0/0.1)#
Verification	● Run the **show running-config** command to display the current configuration status.
	… interface GigabitEthernet 0/0.1 encapsulation dot1Q 100 vlan port 1 2 …

Common Errors

- No 802.1Q VLAN is configured before the command configuration.
- An untagged VLAN fails to be changed to the tag mode because the previous configuration is not deleted by using the **no** form of this command.
- The maximum port ID is less than the minimum port ID for an input port.

2.5.8 Configuring Native VLAN of a Layer-2 Port

Configuration Effect

- Configure the native VLAN of a Layer-2 Port.

Notes

- The native VLANs of all layer-2 ports are VLAN 4089 by default.
- Before the command configuration, run the **vlan port** command to add the ports to the required VLAN (without any tag).

Configuration Steps

- Run the **native vlan** command to complete the configuration.

Verification

- Run the **show running-config** command to display the current configuration status.

Related Commands

Configuring Native VLAN of a Layer-2 Port

Command	**native lan** *num* **vid** *vlan-id*
Parameter Description	*num*: Indicates the port ID. The value range is [0, 4]. *vlan-id:* Indicates the native VLAN to be set.
Command Mode	Global configuration mode
Usage Guide	Run the **no convert lan** *num* command to disable the native VLAN function.

Displaying the Configuration

Command	**show running-config**
Parameter Description	**N/A**
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	N/A

Configuration Example

Configuring Native VLAN 200 for Port 2

Configuration Steps	• Configure Native VLAN 200 for Port 2.
	FS(config)#int gigabitEthernet 0/0.1 FS(config-subif-GigabitEthernet 0/0.1)#encapsulation dot1Q 200 *Oct 23 16:05:10: %7: Command is OK! *Oct 23 16:05:10: %7: Notice: please use command 'vlan port' to add vlan entry. FS(config-subif-GigabitEthernet 0/0.1)#vlan port 2 2 FS(config-subif-GigabitEthernet 0/0.1)#exit FS(config)#native lan 2 vid 200 FS(config)#
Verification	• Run the show **running-config** command to display the configuration result.
	…

Configuration Steps	● Configure Native VLAN 200 for Port 2.
	FS(config)#int gigabitEthernet 0/0.1 FS(config-subif-GigabitEthernet 0/0.1)#encapsulation dot1Q 200 *Oct 23 16:05:10: %7: Command is OK! *Oct 23 16:05:10: %7: Notice: please use command 'vlan port' to add vlan entry. FS(config-subif-GigabitEthernet 0/0.1)#vlan port 2 2 FS(config-subif-GigabitEthernet 0/0.1)#exit FS(config)#native lan 2 vid 200 FS(config)#
Verification	● Run the show **running-config** command to display the configuration result.
	interface GigabitEthernet 0/0.1 encapsulation dot1Q 200 vlan port 2 2 … ! native lan 2 vid 200 ! …

Common Errors

- The port to be set is not a layer-3 port.
- The VLAN to be set does not exist.
- The port to be set is not in the VLAN to be set.
- The VLAN to be set is tagged.

2.5.9 Configuring Layer-2 Port Mirroring

Configuration Effect

- Configure the port mirroring function.

Notes

- The port mirroring function is disabled by default.
- The mirroring port and the mirrored port must be both layer-2 ports.
- There must be only one mirroring port.

Configuration Steps

- Run the **mirror** command to configure the port mirroring function.

Verification

- Run the **show mirror** command to display the configuration result.

Related Commands

Configuring Port Mirroring

Command	**mirror master port** *master_port* **slave port** *slave_port* **{ rx | tx | all }**

Parameter Description	*master_port*: Indicates the mirroring port. The value range is [0, 4]. *slave_port*: Indicates the mirrored port. The value range is [0, 4]. *rx* / *tx* / *all*: Indicates the mirroring mode. There are three mirroring modes: mirroring received packets, mirroring sent packets, and mirroring all packets.
Command Mode	Global configuration mode
Usage Guide	Run the **no mirror master port** *master_port* **slave port** *slave_port* **{ rx | tx | all }** command to disable the port mirroring function.

Displaying Current Configuration

Command	**show mirror**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	N/A

Configuration Example

Mirroring All Packets on Port 1, All Packets Received on Port 2, and All Packets Sent on Port 3 to Port 0

Configuration Steps	● Mirror all packets on Port 1, all packets received on Port 2, and all packets sent on Port 3 to Port 0.
	FS(config)#mirror master port 0 slave port 1 all FS(config)#mirror master port 0 slave port 2 rx FS(config)#mirror master port 0 slave port 3 tx FS(config)#
Verification	● Run the **show** command to display the configuration result.
	master: 0 slave: 1(all) 2(rx) 3(tx)

Common Errors

- The mirroring port or the mirrored port is not a layer-2 port.
- The current mirroring port is different from the previously configured mirroring port.
- The mirroring port and the mirrored port are the same.

2.5.10 Configuring Switching Between 40GE and 10GE Ports

Configuration Effect

- Switch between one 40GE port and four 10GE ports.

Notes

- The configuration can take effect only after the device is restarted.

Configuration Steps

- Run the **split** command in global configuration mode to switch between the 40GE port and 10GE ports.

Verification

- Restart the device and display the interface information.

Related Commands

Configuring 10GE Port Mode

Command	**split slot** *slot-num*
Parameter Description	*slot-num*: Indicates the slot ID of the 40GE port to be switched. The value range is [0, 1].
Command Mode	Global configuration mode
Usage Guide	Run the ***no** form of this command to disable the 10GE port mode.

Displaying Current 10GE Port Mode

Command	**show interface**
Parameter Description	**N/A**
Command Mode	Privileged EXEC Mode
Usage Guide	N/A

Configuration Example

Switching the First 40GE Port into Four 10GE Ports

Configuration Steps	• Switch the first 40GE port into four 10GE ports.
	FS(config)#split slot 0 Please save the config, and reload system to take effect!
Verification	• Save the configuration, restart the device, and run the **show** command to display the configuration result.
	FS#show interface … ========== TenGigabitEthernet 0/8 ========== … ========== TenGigabitEthernet 0/9 ========== … ========== TenGigabitEthernet 0/10 ========== … ========== TenGigabitEthernet 0/11 ========== …

2.6 Monitoring

Displaying

Description	Command

Displays information about the system mode and the internal and external network attributes of interfaces.	**show sys-mode**
Displays information about the bridge-map. In one-armed mode, you can also display information about the configured IP address segment of the internal network.	**show bridge-map** *bridge-num* [**lan-ip**]

3 Configuring DLDP

3.1 Overview

The Data Link Detection Protocol (DLDP) is a protocol used to quickly detect faulty Ethernet links.

A typical Ethernet link detection mechanism detects physical link connectivity through autonegotiation at the physical layer. Such a mechanism has limitations when detecting Layer-3 data communication exceptions despite normal physical connections.

DLDP provides reliable Layer-3 link detection information. After detecting a faulty link, DLDP shuts down the logical state of Layer-3 ports to realize fast Layer-3 protocol convergence.

3.2 Applications

Application	Description
Intra-Network Segment DLDP Detection	The source IP address of the detected port and the detected IP address are in the same network segment.
Inter-Network Segment DLDP Detection	The source IP address of the detected port and the detected IP address are in different network segments.

3.2.1 Intra-Network Segment DLDP Detection

Scenario

This section describes the basic DLDP application scenario where the source IP address of the detected port and the detected IP address are in the same network segment.

In Figure 3- 3- 1, the Gi 0/1 Layer-3 port on Switch A and the Gi 0/2 Layer-3 port on Switch C are in the same network segment. To detect the Layer-3 link connectivity from Gi 0/1 to Gi 0/2, enable DLDP on Gi 0/1 or Gi 0/2.

Figure 3- 3- 1

Remarks	Device A and Device C are switches. Gi 0/1 and Gi 0/2 are Layer-3 ports in the same network segment. B is a network in the same network segment as Gi 0/1 and Gi 0/2.

Deployment

- Enable DLDP on Gi 0/1 or Gi 0/2.

3.2.2 Inter-Network Segment DLDP Detection

Scenario

This section describes the DLDP application scenario where the source IP address of the detected port and the detected IP address are in different network segments.

In Figure 3- 3- 2, the Gi 0/1 Layer-3 port on Switch A and the Gi 0/4 Layer-3 port on Switch D are in different network segments. To detect the Layer-3 link connectivity from Gi 0/1 to Gi 0/4, enable DLDP on Gi 0/1 and configure the DLDP next-hop IP address (IP address of the Gi 0/2 port on Switch B).

Figure 3- 3- 2

Remarks	Device A, Device B, and Device D are switches. Gi 0/1 and Gi 0/4 are Layer-3 ports in different network segments.

Deployment

- Enable DLDP on Gi 0/1 and configure the DLDP next-hop IP address.

3.3 Features

Basic Concepts

DLDP Detection Interval and Retransmission Times

Detection interval: Indicates the interval at which DLDP detection packets (ICMP echo) are transmitted.

Retransmission times: Indicate the maximum times DLDP detection packets can be retransmitted in the case of a DLDP detection failure. When a network device does not receive a reply packet from the peer end within the period of the detection interval multiplied by the retransmission times, the device determines that a Layer-3 link failure occurs and shuts down the logical state of its Layer-3 port (despite the normal physical link connection). When Layer-3 link connectivity is recovered, the device restores its Layer-3 port to Up logical state.

DLDP Detection Modes

Active mode and passive mode are two DLDP detection modes.

Active mode (default): ICMP detection packets are sent actively.

Passive mode: ICMP detection packets are received passively.

DLDP Next Hop

Next hop: Indicates the next node connected to the detected IP address in inter-network segment DLDP detection.

In some cases, DLDP needs to detect IP reachability in non-directly connected network segments. You need to configure the next-hop IP address for the detected port to allow DLDP to obtain the next-hop MAC address through an ARP packet before sending a correct ICMP packet.

In this situation, you need to avoid the return of the reply packet from another link; otherwise, DLDP will misjudge that the detected port does not receive an ICMP reply.

DLDP Recovery Times

Recovery times: Indicate the times DLDP needs to receive consecutive reply packets (ICMP reply) before it can determine link failure recovery.

In some cases, link detection may be unstable. For example, a link is only intermittently pingable. In this case, DLDP repeatedly changes the link status between Up and Down, which may further destabilize the ring network.

Recovery times indicate the times DLDP needs to receive consecutive reply packets before DLDP can set the link in Down state to Up. The default recovery times are three times, indicating that the link needs to be successfully pinged three times before it is set to Up. The recovery times setting reduces link detection sensitivity but increases stability. Related parameters are adjustable according to the network condition.

DLDP Bound MAC Address

Bound MAC address: Indicates the MAC address bound to the detected IP address.

In a complex network environment, DLDP may obtain an invalid MAC address if the detected link has abnormal ARP packets transmitted (causing ARP spoofing), which will make DLDP detection abnormal.

To address this problem, you can bind the detected IP address (or next-hop IP address) to a static MAC address to avoid a DLDP failure in the case of ARP spoofing.

Overview

Feature	Description
DLDP Detection	Detects Layer-3 link connectivity. When a Layer-3 link is abnormal, DLDP shuts down the Layer-3 port.
MAC Address Binding	Binds the detected IP address to the MAC address of the detected device to avoid DLDP exceptions otherwise caused by ARP spoofing.
Passive DLDP Detection	When both ends of the detected link are enabled with DLDP, you can configure one end in passive mode to save bandwidth and CPU resources.

3.3.1 DLDP Detection

DLDP detects Layer-3 link connectivity. When a Layer-3 link is abnormal, DLDP shuts down the corresponding Layer-3 port.

Working Principle

After DLDP detection is enabled, DLDP sends an ARP packet to obtain the MAC address and outbound port of the detected device or the next-hop device. Then DLDP periodically sends IPv4 ICMP echo packets to the MAC address and outbound port to detect link connectivity. If DLDP does not receive an IPv4 ICMP reply packet from the detected device within a specific period, DLDP determines that the link is abnormal and sets the Layer-3 port to Down.

Related Configuration

- Enabling DLDP Detection

By default, DLDP detection is disabled on ports.

Run the **dldp** command with the detected IP address specified to enable DLDP detection.

You can configure the next-hop IP address, MAC address of the detected device, transmission interval, retransmission times, and recovery times based on the actual environment.

3.3.2 MAC Address Binding

The MAC address binding feature is used to bind the detected IP address (or next-hop IP address) to the MAC address of the detected device (or next-hop device) to avoid DLDP exceptions otherwise caused by ARP spoofing

Working Principle

You can bind the detected IP address (or next-hop IP address) to a static MAC address to avoid a DLDP failure in the case of ARP spoofing.

Related Configuration

By default, no MAC address is bound in DLDP detection.

Bind the MAC address of the detected device when you run the **dldp** command to enable DLDP detection. If the next-hop IP address is specified, bind the MAC address of the next-hop device.

After DLDP detection is enabled, DLDP sends ARP packets and ICMP packets with a fixed destination IP address and a fixed destination MAC address. If the source IP address and MAC address in the received packet do not match the bound IP address and MAC address, DLDP will not process the packet.

3.3.3 Passive DLDP Detection

When both ends of the detected link are enabled with DLDP, you can configure one end in passive mode to save bandwidth and CPU resources.

Working Principle

After the device at the local end sends an ICMP echo packet, the peer device determines link connectivity according to the packet reception time by using specific detection parameters, which are the same as those at the local end, thus saving bandwidth and CPU resources.

Related Configuration

By default, passive DLDP detection is disabled.

Run the **dldp passive** command to enable passive DLDP detection.

After passive DLDP detection is enabled, DLDP will return an ICMP reply packet upon receiving an ICMP echo packet, instead of actively sending ICMP echo packets to the peer end. If DLDP does not receive an ICMP echo packet within a specific period, it determines that the link to the peer port is abnormal.

3.4 Configuration

Configuration	Description and Command	
Enabling DLDP Detection	(Mandatory) It is used to enable DLDP detection in interface configuration mode.	
	dldp	Enables DLDP detection.
	(Mandatory) It is used to enable passive DLDP detection in interface configuration mode.	
	dldp passive	Enables passive DLDP detection.
	(Optional) It is used to configure the detection interval, retransmission times, and recovery times of DLDP detection in global configuration mode.	
	dldp interval	Modifies the DLDP parameters globally to apply the modifications to DLDP detection on all ports.
	dldp retry	
	dldp resume	

3.4.1 Enabling DLDP Detection

Configuration Effect

- Detect Layer-3 link connectivity. When a Layer-3 link is abnormal, DLDP shuts down the Layer-3 port.

Notes

- DLDP supports the configuration of multiple IP addresses on a Layer-3 port. DLDP sets the port to Down when none of the IP addresses receives an ICMP reply. If one IP address resumes communication, DLDP sets the port to Up again.
- DLDP uses the first IP address of the Layer-3 port as the source IP address of detection packets.

Configuration Steps

Enabling DLDP Detection

- Mandatory.
- When you enable DLDP detection in interface configuration mode, you can configure the next-hop IP address, MAC address, transmission interval, retransmission times, and recovery times based on the actual environment.

Configuring a DLDP Detection Mode

- Optional.
- You can configure active or passive DLDP detection in interface configuration mode based on the actual environment.
- If DLDP detection needs to be enabled at both ends of a Layer-3 link, you can configure passive DLDP detection at one end to save bandwidth and CPU resources.

Configuring DLDP Parameters Globally

- Optional.
- You can modify the parameters of DLDP detection on all ports in global configuration mode based on requirements. The parameters include the packet transmission interval, packet retransmission times, and recovery times.

Verification

- Display the device DLDP information, including the status and statistics of DLDP detection on all ports.

Related Commands

Enabling DLDP Detection

Command	**dldp** *ip-address* [*next-hop-ip*] [**mac-address** *mac-addr*] [**interval** *tick*] [**retry** *retry-num*] [**resume** *resume-num*]
Parameter Description	*ip-address*: Indicates the detected IP address. ***next-hop-ip***: Indicates the next-hop IP address. *mac-addr*: Indicates the MAC address of the detected device to be bound. If the next-hop IP address is specified, bind the MAC address of the next-hop device. *tick*: Indicates the interval at which detection packets are transmitted. The value ranges from 5 to 6,000 ticks (1 tick = 10 ms). The default value is 100 ticks (1s). *retry-num*: The value ranges from 1 to 3,600. The default value is 4. *resume-num*: Indicates the recovery times. The value ranges from 1 to 200. The default value is 3.
Command Mode	Interface configuration mode
Usage Guide	The port to be enabled with DLDP detection must be a Layer-3 port, such as a router port, L3AP port, and SVI port.

Configuring a DLDP Detection Mode

Command	**dldp passive**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	You need to enable DLDP detection before configuring a DLDP detection mode.

Modifying DLDP Detection Parameters Globally

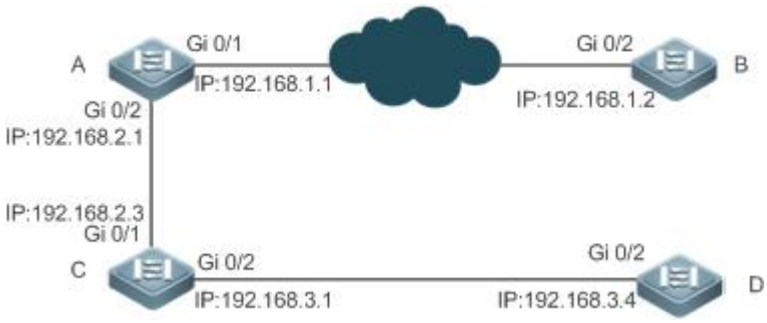
Command	**dldp** { **interval** *tick* | **retry** *retry-num* | **resume** *resume-num* }
Parameter Description	*tick*: Indicates the interval at which detection packets are transmitted. The value ranges from 5 to 6,000 ticks (1 tick = 10 ms). The default value is 100 ticks (1s). *retry-num*: Indicates the interval at which detection packets are retransmitted. The value ranges from 5 to 3,600. The default value is 4. *resume-num:* Indicates the recovery times. The value ranges from 1 to 200. The default value is 3.
Command Mode	Global configuration mode
Usage Guide	Use this command to quickly modify the parameters of DLDP detection on all ports when the actual environment is changed.

Displaying the DLDP Status

Command	**show dldp statistic** [**interface** *interface-name*]
Parameter Description	*interface-name*: Indicates the Layer-3 port on which the DLDP status will be displayed.
Command Mode	Privileged mode, global configuration mode, and interface configuration mode
Usage Guide	Use this command to display the DLDP status on a specific port. You can also use this command to display the DLDP status on all ports.

Configuration Example

Enabling DLDP Detection on Layer-3 Ports on Device A and Device B in a Layer-3 Network

Scenario **Figure 3- 3- 3**	
	
Verification	● Enable DLDP detection on the Gi 0/1 and Gi 0/2 router ports on Device A to detect the Layer-3 link connectivity between Device A and Device B and that between Device A and Device D. ● To control the Gi 0/2 router port of Device B, enable passive DLDP detection on the port.
A	A#configure terminal A(config)#interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#dldp 192.168.1.2 A(config-if-GigabitEthernet 0/1)# exit A(config)#interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/1)#dldp 192.168.3.4 192.168.2.3
B	B#configure terminal B(config)#interface GigabitEthernet 0/2 B(config-if-GigabitEthernet 0/1)#dldp 192.168.1.1 B(config-if-GigabitEthernet 0/1)#dldp passive
Verification	● Display the DLDP status on Device A and Device B to check whether DLDP detection is enabled and works normally.
A	A# show dldp Interface Type Ip Next-hop Interval Retry Resume State --------- ------- ----------- ----------- -------- ----- ------ ------ Gi0/1 Active 192.168.1.2 100 4 3 Up Gi0/1 Active 192.168.3.4 192.168.2.3 100 4 3 Up
B	B# show dldp Interface Type Ip Next-hop Interval Retry Resume State --------- ------- ----------- ----------- -------- ----- ------ ------

	Gi0/2	Passive	192.168.1.1	100	4	3	Up

Common Errors

- An unreachable IPv4 unicast route is misjudged as a DLDP detection failure.
- DLDP detection fails because the peer device does not support ARP/ICMP replies.
- No next-hop IP address is configured in inter-network segment DLDP detection.

3.5 Monitoring

Clearing

Description	Command
Clears DLDP statistics.	**clear dldp** [**interface** *interface-name* [*ip-address*]]

Displaying

Description	Command
Displays the DLDP status.	**show dldp** [**interface** *interface-name*]
Displays the DLDP statistics on the Up/Down port sates.	**show dldp statistic**

4 Configuring PCAP

4.1 Overview

Packet Capture (PCAP) is a maintenance function commonly used in network devices.

Similar to the packet capture software running on a personal computer, the PCAP function can capture, save, or display the packets sent from and received by the network device.

4.2 Applications

Application	Description
Capturing Packets	

4.2.1 Capturing Packets

Scenario

During routine maintenance, if you find packet sending or receiving failures in the network, specify the capture point and capture direction, enter the packet feature, and start the packet capture to check whether the packets arrives at the device or are sent from the device.

Deployment

Perform packet capture as follows:

- Create a capture feature rule and name it.
- Create a capture point and specify the capture point name, capture location (physical port, VLAN, and control plane), capture direction, and capture feature.
- Specify the name of the file to be saved.
- Enable packet capture at the capture point.
- Wait until the capture ends.
- Upload the file to the PC.
- Enable the capture software on the PC to check the captured packets.

4.3 Features

Overview

Feature	Description
Capturing Packets	Captures packets sent and received on a specified physical port, VLAN, and control plane.

4.3.1 Capturing Packets

Clients can define the capture point and specify the capture location and direction, matching rule information, number of captured packets, and file name; and then enable the capture procedure.

Working Principle

Clients can define the capture rules by defining capture points. To capture multiple types of packets at the same time, a client is allowed to define multiple capture points and distinguish them by their names. The capture rules are as follows:

1) The capture location can be selected from the certain physical port, VLAN port, and system control plane. Each capture point can only have one capture location.
2) The available capture directions can be the outgoing direction, incoming direction, and bidirectional.
3) The 7-tuple information can match the source MAC address, destination MAC address, layer-2 protocol type, source IP address, destination IP address, layer-3 protocol type, and TCP/UDP port information.
4) The number of captured packets or size of the captured packet can be specified.
5) The file name can be specified. The captured packet will be saved in PCAP file format. The file will be output in the form of system log by default on the console unless otherwise specified.

A client enables capture via commands after the rules are configured. The capture will automatically stop when the number of captured packets or the file size reaches the specified value. The client can also stop the capture after commands are entered manually.

Due to too many packets displayed, only 30 packets will be displayed in the form of system log on the console by default if the file name is not specified.

4.4 Configuration

Configuration	Description and Command	
Capturing Packets	**packet capture rule** *rule-name* **[src-mac** *smac*] **[dst-mac** *dmac*] **[etype** *type* | **ip** | **arp**] **[src-ip** *sip sip-mask*] **[dst-ip** *dip dip-mask*] **[protocol** *protocol* | **tcp** | **udp]** **[src-port** *sport*] **[dst-port** *dport*]	Defines capture matching rule.
	packet capture point *capture-point-name* **rule** *rule-name* **location {interface** *interface-name* | **vlan** *vlan-id* | **control-plane} {in | out | both}**	Creates the capture point and specifies the capture location, matching rule, and capture direction.
	packet capture file *filename* **[buffer-size** *buf-size*] **[packet-num** *pkt-num*]	Specifies the name of the file to be saved.
	packet capture {start | stop}	Starts/Stops packet capture.

4.4.1 Capturing Packets

Configuration Effect

- Define the capture matching rule.
- Create the capture point.
- Specify the name of the file to be saved.
- Start packet capture.
- Stop packet capture.

Configuration Steps

Defining Capture Matching Rule

- (Mandatory) Run this command to define the packet capture rule.

Command	**packet capture rule** *rule-name* **[src-mac** *smac*] **[dst-mac** *dmac*] **[etype** *type* | **ip** | **arp**] **[src-ip** *sip sip-mask*] **[dst-ip** *dip dip-mask*] **[protocol** *protocol* | **tcp** | **udp]** **[src-port** *sport*] **[dst-port** *dport*]
Parameter Description	*rule-name*: Indicates the matching rule name. *smac*: Indicates the source MAC address. *dmac*: Indicates the destination MAC address. *type* | **ip** | **arp**: Indicates the layer-2 protocol type.

	sip: Indicates the source IP address. *sip-mask*: Indicates the source IP address mask. *dip*: Indicates the destination IP address. *dip-mask*: Indicates the destination IP address mask. *protocol* **| tcp | udp**: Indicates the layer-3 protocol type. *sport*: Indicates the TCP/UDP protocol source port. *dport*: Indicates the TCP/UDP protocol destination port.
Defaults	-
Command Mode	Privileged EXEC mode
Usage Guide	1. The user can define multiple capture rules and distinguish them by different names. After a rule is defined, the rule needs to be referenced by the packet capture point to actually take effect. 2. Before deleting the capture rule, all the packet capture points referencing the rule need to be deleted.

Creating Capture Point

- (Mandatory) Run this command to create the capture point.

Command	**packet capture point** *capture-point-name* **rule** *rule-name* **location {interface** *interface-name* | **vlan** *vlan-id* | **control-plane} {in | out | both}**
Parameter Description	*capture-point-name*: Indicates the capture point name. *rule-name*: Indicates the matching rule name, which is defined by running the **packet capture rule** command. *interface-name*: Indicates the name of the port on which packets are captured. *vlan-id*: Indicates the ID of the VLAN in which packets are captured. control-plane: Indicates the control plane on which packets are captured. **in | out | both**: Indicates the capture direction (incoming, outgoing, or bidirectional).
Defaults	-
Command Mode	Privileged EXEC mode
Usage Guide	1. The user can define multiple capture points at the same location as required to match different capture rules or packet directions. The capture points can work simultaneously without affecting each other. 2. If the capture point is modified during packet capture, the modification will not take effect immediately and will take effect next time when packet capture is enabled.

Specifying Name of File to Be Saved

- (Optional) Run this command to specify the name of the file to be saved.

Command	**packet capture file** *filename* **[buffer-size** *buf-size***] [packet-num** *pkt-num***]**
Parameter Description	*filename*: Indicates the name of the file to be saved. *buf-size*: Indicates the buffer size. The buffer size is 2 MB by default if not specified. Packet capture automatically stops when the buffer is full. *pkt-num*: Indicates the number of captured packets. Packet capture automatically stops when the number of captured packets reaches the specified number. Packets will be captured continually by default unless otherwise specified.
Defaults	-
Command Mode	Privileged EXEC mode

Usage Guide	1. The packet data is saved in the file by default after the file name is set. If no file name is set, the data is directly output on the console in the form of system log. Only 30 packets can be output by default when no file name is set. 2. The file name setting takes effect next time when packet capture is enabled.

Starting/Stopping Packet Capture

- (Mandatory) Enter this command to start or stop packet capture.

Command	**packet capture {start | stop}**
Parameter Description	**start | stop**: Starts/Stops packet capture.
Defaults	-
Command Mode	Privileged EXEC mode
Usage Guide	1. If the packet capture stop command is not entered after packet capture starts, the packet capture automatically stops at the capture point when the number of captured packets reaches the specified number. If the packet capture stop condition is not met, run this command to immediately stop the packet capture. 2. Run the packet capture start command to capture packets at all packet capture points simultaneously.

Verification

Run the **show packet capture status** command to display packet capture information.

Command	**show packet capture status**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Run this command to display the packet capture status.

Command Presentation	FS#show packet capture status
	
	Capture rules:
	  Capture rules tcp:
	  etype: 0x0800
	  source MAC: 2222.2222.2222
	  destination MAC: 1111.1111.1111
	  protocol: 0x6
	  source IP: 10.10.10.3
	  destination IP: 10.10.10.10
	  source port: 5
	  destination port: 10
	
	Capture points:
	  Capture point controlplane:
	  Capture rules: tcp
	  location: control-plane
	  direction: all
	  status: stopped

```
            packets captured(in): 200
            packets captured(out): 200

Capture file:
      Filename: /tmp/tcp.pcap
            Buffer size: 2(MB)
            packets limit: 500
FS#
```

Configuration Example

Capturing Packets

Scenario	● In the client environment, the TCP connection of a certain application on a device connected to Port 0/1 fails, TCP packets need to be captured on this port for analysis.
Configuration Steps	● Run the packet capture command to capture and save TCP packets to the file tcp.pcap and upload the file to a PC to display the captured data.
	FS# packet capture rule tcp etype ip protocol tcp FS# packet capture point tcppoint rule tcp location interface gi0/1 both FS# packet capture file flash:tcp.pcap packet-num 1500 FS# packet capture start

Verification	0FS#show packet capture status
	
	Capture rules:
	  Capture rules tcp:
	  etype: 0x0800
	  protocol: 0x6
	
	Capture points:
	  Capture point tcppoint:
	  Capture rules: tcp
	  location: Gi0/1
	  direction: all
	  status: running
	  packets captured(in): 550
	  packets captured(out): 550
	
	Capture file:
	  filename: /data/tcp.pcap
	  buffer size: 2(MB)
	  packets limit: 1500

4.5 Monitoring

Displaying

Description	Command
Displays the packet capture status.	**show packet capture status**

5 Configuring PPPOE-CLIENT

5.1 Overview

PPPoE: Point-to-point Protocol Over Ethernet

FS products support the PPPoE client on Ethernet interfaces, and are therefore able to connect to a host network by accessing a remote hub through a simple access device. The PPPoE protocol enables the PPPoE server to control each access client and perform relevant accounting.

FS products support the auto dialing mode: no Dial-on-Demand Routing (DDR) but always online.

- The PPPoE client is applicable in scenarios where Internet access is implemented through ADSL.

The following sections describe the PPPoE client only.

5.2 Applications

Application	Description
ADSL Scenario	In a scenario where Internet access is implemented through the Asymmetric Digital Subscriber Line (ADSL) technology, the device provides dialup and packet forwarding functions.

5.2.1 ADSL Scenario

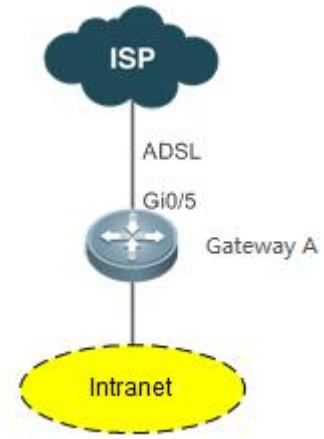
Scenario

In a scenario where Internet access is implemented through ADSL, the device provides dialup and packet forwarding functions.

The dialup networking scenario is illustrated with Figure 5- 5- 1 as an example.

- The dialup function is enabled on the device. The device connects to a remote Internet service provider (ISP) over an ADSL line, and obtains Internet access capability.
- Intranet PCs access the Internet through the device.

Figure 5- 5- 1



Corresponding Protocols

- Enable the dialup function on the device, and dial up to the Internet over the ADSL line.

5.3 Features

Basic Concepts

- **ISP**

A network operator who provides users with Internet access service, information service, and value-added services (VASs).

- **ADSL**

It indicates a line on which users dial up to the Internet.

- **Data Flow**

It indicates a flow of packets only forwarded by the device.

- **Interested Flow**

It indicates a specific type of packets defined by users during configuration, which can trigger the device to start dialup.

Overview

Feature	Description
Dialup to the Internet	In a scenario where Internet access is implemented through the Asymmetric Digital Subscriber Line (ADSL) technology, the device provides dialup and packet forwarding functions.

5.3.1 Dialup to the Internet

The device has Internet access capability after the dialup is complete; therefore, hosts in the intranet also have Internet access capability.

Working Principle

Dialup corresponds to the negotiation process, whereas Internet access corresponds to the packet forwarding process.
Negotiation can be further divided into three parts: protocol negotiation, protocol keepalive, and protocol termination.

- **Protocol Negotiation**

Protocol negotiation is divided into PPPoE negotiation and PPP negotiation.
During PPPoE negotiation, both parties confirm a unique peer, record the peer's MAC address, and establish a unique session ID.
During PPP negotiation, the server checks the client's authentication information. If the client passes the authentication, the server allocates an IP address to the client. If the client has already been configured with an IP address and the configured IP address meets the server's requirements, the server will agree to use this IP address as the IP address of the client.
After both protocols are up, the device has Internet access capability and prepares a Layer 2 (L2) header that is necessary for data packet encapsulation.

- **Protocol Keepalive**

After PPP is up, both parties periodically send LCP heartbeat packets to each other. If the party at one end does not receive any heartbeat response from the other party, it actively terminates the protocol.

- **Protocol Termination**

In certain cases, either party may actively terminate the protocol.
The initiating party sends a PPP termination packet to end the current PPP session, and then sends a PPPoE termination packet to end the current PPPoE session.
After receiving the PPP termination packet, the passive party returns an acknowledgement packet to agree to the termination of the PPP session; and after receiving the PPPoE termination packet, the passive party returns another acknowledgement packet to agree to the termination of the PPPoE session.

Once either party receives a PPPoE termination protocol, the PPP session and the PPPoE session will immediately terminate, even if it has not received any PPP termination protocol.

Packet Forwarding

Packet sending process: When a data packet is routed to the dialer interface, the device encapsulates the data packet with the prepared L2 header information and ultimately sends the data packet from a physical port.

Packet receiving process: After a packet arrives at a physical port, the device marks the Layer 3 (L3) header position of the packet, executes the next service, and ultimately sends the packet to a host in the intranet.

Related Configuration

Configuring the Ethernet Interface

By default, the following functions are disabled and there is no corresponding default value.

Run the **pppoe enable** command to enable the PPPoE client function on the interface.

Run the **no pppoe enable** command to disable the PPPoE client function on the interface.

Run the **pppoe-client dial-pool-number** *pool-number* **no-ddr** command to bind the Ethernet interface to a specific logical dialer pool. The logical dialer pool provides automatic dialing and is always online.

Run the **no pppoe-client dial-pool-number** *pool-number* command to unbind the Ethernet interface from the specific logical dialer pool.

Run the **pppoe session mac-address** *H.H.H* command to configure the MAC address of the PPPoE session.

Configuring the Logical Interface

By default, the following functions are disabled.

Run the **interface dialer** *dialer-number* command to add a specific logical interface and enter the configuration mode of the logical interface.

Run the **no interface dialer** *dialer-number* command to delete the specific logical interface.

Run the **ip address negotiate** command to configure negotiation-based IP address acquisition.

Run the **no ip address negotiate** command to remove the configuration of negotiation-based IP address acquisition.

Run the **dialer pool** *number* command to associate a dialer pool, which corresponds to the dialer pool configured on the Ethernet interface.

Run the **no dialer pool** *number* command to remove the association with the dialer pool.

Run the **encapsulation ppp** command to configure the encapsulation protocol PPP. PPPoE is established on the basis of PPP.

Run the **no encapsulation** command to remove the encapsulation protocol configuration.

Run the **mtu** *1488* command to set the Maximum Transmit Unit (MTU) to 1488.

Run the **no mtu** command to remove the MTU configuration.

Run the **dialer-group** *dialer-group-number* command to associate a dialer triggering rule, which corresponds to the dialer-list.

Run the **no dialer-group** command to remove the configuration of the dialer triggering rule.

Run the **ppp chap hostname** *username* command to configure the user name for CHAP authentication.

Run the **no ppp chap hostname** command to remove the user name configuration for CHAP authentication.

Run the **ppp chap password** *password* command to configure the password for CHAP authentication.

Run the **no ppp chap password** command to remove the password configuration for CHAP authentication.

Run the **ppp pap sent-username** *username* **password** *password* command to configure the user name and password for PAH authentication.

Run the **no ppp pap sent-username** command to remove the user name and password configuration for PAH authentication.

Configuring Mandatory Global Parameters

By default, the following functions are disabled and shall be configured according to actual requirements. If other functional modules need to be used together, you also need to configure other global parameters.

Run the **dialer-list number protocol** *protocol-name* **ip**{ **permit** | **deny** | **list** *access-list-number*} command to define a dialer triggering rule.

Run the **no dialer-list number** command to delete the configured dialer triggering rule.

Run the **ip route** *0.0.0.0 0.0.0.0* **dialer** *dialer-number* [**permanent**] command to configure a route. If you specify the **permanent** option, the route will be always valid, even if the logical interface is within the enable-timeout period, in which case the logical interface will be down.

Run the **no ip route** *0.0.0.0 0.0.0.0* **dialer** *dialer-number* command to remove the route.

5.4 Limitations

EG2000CE supports multi-dial; EG3000XE and EG3000UE do not support multi-dial.

5.5 Configuration

Configuration	Description and Command	
Configuring Basic Functions of the PPPoE Client	Mandatory configuration.	
	pppoe enable	Enables the PPPoE client function.
	pppoe-client dial-pool-number *number* **no-ddr**	Binds a logical dialer pool and specifies the dialing mode.
	pppoe session mac-address *H.H.H*	Configures the MAC address of the PPPoE session.
	interface dialer *dialer-number*	Adds a specific logical interface and enters the configuration mode of the logical interface.
	ip address { **negotiate** | *ip-addr subnet-mask* }	Configures the IP address acquisition mode.
	dialer pool *number*	Associates a dialer pool.
	encapsulation ppp	Configures the encapsulation protocol PPP.
	mtu *1488*	Sets the MTU to 1488.
	dialer-group *dialer-group-number*	Associates a dialer triggering rule.
	ppp chap hostname *username*	Configures the user name for CHAP authentication.
	ppp chap password *password*	Configures the password for CHAP authentication.
	ppp pap sent-username *username* **password** *password*	Configures the user name and password for PAP authentication.
	dialer-list number protocol *protocol-name* **ip** { **permit** | **deny** | **list** *access-list-number* }	Defines a dialer triggering rule.

5.5.1 Configuring Basic Functions of the PPPoE Client

Networking Requirements

- The device initiates PPPoE negotiation, and completes the negotiation process, protocol keepalive, and protocol termination.

- The device obtains Internet access capability after the negotiation is complete, and starts to forward a data flow which is routed to the dialer interface.

Notes

- After the kernel module is uninstalled, users can still perform configuration management but negotiation and data flow forwarding cannot be performed.

Configuration Steps

Enabling the PPPoE Client Function

- The configuration is mandatory.
- Perform this configuration in Ethernet interface configuration mode.
- Enable the PPPoE client function.

Binding a Logical Dialer Pool and Specifying the Dialing Mode

- The configuration is mandatory.
- Perform this configuration in Ethernet interface configuration mode.
- Bind the Ethernet interface to a specific logical dialer pool and specify the dialer mode.

Configuring the MAC Address of the PPPoE Session

- The configuration is mandatory.
- Perform this configuration in Ethernet interface configuration mode.
- Specify the MAC address of the PPPoE session for subinterface dialing.

Adding a Specific Logical Interface and Entering the Configuration Mode of the Logical Interface

- The configuration is mandatory.
- Perform this configuration in global configuration mode.
- Add a specific logical interface and enter its configuration mode.

Configuring the Way of Acquiring the IP Address of the Logical Interface

- The configuration is mandatory.
- Perform this configuration in logical interface configuration mode.
- Configure the way of acquiring the IP address of the logical interface.

Associating a Dialer Pool

- The configuration is mandatory.
- Perform this configuration in logical interface configuration mode.
- Associate the logical interface with a specific dialer pool.

Configuring the Encapsulation Protocol

- The configuration is mandatory.
- Perform this configuration in logical interface configuration mode.
- Configure the encapsulation protocol PPP on the logical interface.

Configuring the MTU of the Logical Interface

- The configuration is mandatory.
- Perform this configuration in logical interface configuration mode.
- Set the MTU of the logical interface to 1488.

Associating a Dialer Triggering Rule

- The configuration is mandatory.
- Perform this configuration in logical interface configuration mode.

- Associate a dialer triggering rule.

Configuring the User Name for CHAP Authentication

- The configuration is mandatory.
- Perform this configuration in logical interface configuration mode.
- Configure the user name for CHAP authentication.

Configuring the Password for CHAP Authentication

- The configuration is mandatory.
- Perform this configuration in logical interface configuration mode.
- Configure the password for CHAP authentication.

Configuring the User Name and Password for PAP Authentication

- The configuration is mandatory.
- Perform this configuration in logical interface configuration mode.
- Configure the user name and password for PAP authentication.

Defining a Dialer Triggering Rule

- The configuration is mandatory.
- Perform this configuration in global configuration mode.
- Define a dialer triggering rule.

Verification

- Check whether the dialer interface has acquired an IP address.
- Check whether a correct dialer interface route entry has been established on the device.

Related Commands

Enabling the PPPoE Client Function

Command Syntax	**pppoe enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Configuration Usage	The interface on which the PPPoE client will be enabled must be a WAN Ethernet interface.

Binding a Logical Dialer Pool and Specifying the Dialing Mode

Command Syntax	**pppoe-client dial-pool-number** *number* **no-ddr**
Parameter Description	*number*: number of the dialer pool
Command Mode	Interface configuration mode
Configuration Usage	The PPPoE client function must be enabled on the interface first.

Configuring the MAC Address of the PPPoE Session

Command Syntax	**pppoe session mac-address** *H.H.H*
Parameter Description	*H.H.H*: MAC address
Command Mode	Interface configuration mode

Configuration Usage	The PPPoE client function must be enabled on the subinterface first.

Adding a Specific Logical Interface and Entering its Configuration Mode

Command Syntax	**interface dialer** *dialer-number*
Parameter Description	*dialer-number*: interface number
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuring the Way of Acquiring the IP Address of the Logical Interface

Command Syntax	**ip address** { **negotiate** | *ip-addr subnet-mask* }
Parameter Description	*ip-addr*: manually configured IP address *subnet-mask*: manually configured subnet mask
Command Mode	Interface configuration mode
Configuration Usage	If you select **negotiate**, the IP address of the dialer interface will be acquired through negotiation. If you manually specify the IP address of the dialer interface, the peer's consent is required during negotiation for the device to work properly.

Associating a Dialer Pool

Command Syntax	**dialer pool** *number*
Parameter Description	*number*: number of the dialer pool
Command Mode	Interface configuration mode
Configuration Usage	An Ethernet interface will be selected from the dialer pool as the dialer interface to perform dialing.

Configuring the Encapsulation Protocol

Command Syntax	**encapsulation ppp**
Parameter Description	N/A
Command Mode	Interface configuration mode
Configuration Usage	N/A

Configuring the MTU of the Logical Interface

Command Syntax	**mtu** *1488*
Parameter Description	N/A
Command Mode	Interface configuration mode
Configuration Usage	Because Internet access is implemented through the PPPoE protocol, the L2 header of a packet is longer than that of a common Ethernet packet.

Associating a Dialer Triggering Rule

Command Syntax	**dialer-group** *dialer-group-number*
Parameter	*dialer-group-number*: number of the dialer triggering rule

Description	
Command Mode	Interface configuration mode
Configuration Usage	If the DDR mode is specified, the device will be triggered to perform dialing only when a packet meeting the rule is routed to the dialer interface. If the no-DDR mode is specified, the configuration will not take effect on the device.

Configuring the User Name for CHAP Authentication

Command Syntax	**ppp chap hostname** *username*
Parameter Description	*username*: user name
Command Mode	Interface configuration mode
Configuration Usage	N/A

Configuring the Password for CHAP Authentication

Command Syntax	**ppp chap password** *password*
Parameter Description	*password*: password
Command Mode	Interface configuration mode
Configuration Usage	N/A

Configuring the User Name and Password for PAP Authentication

Command Syntax	**ppp pap sent-username** *username* **password** *password*
Parameter Description	*username*: user name *password*: password
Command Mode	Interface configuration mode
Configuration Usage	N/A

Defining a Dialer Triggering Rule

Command Syntax	**dialer-list number protocol** *protocol-name* **ip**{ **permit** | **deny** | **list** *access-list-number* }
Parameter Description	*protocol-name*: protocol name *access-list-number*: ACL number
Command Mode	Global configuration mode
Configuration Usage	N/A

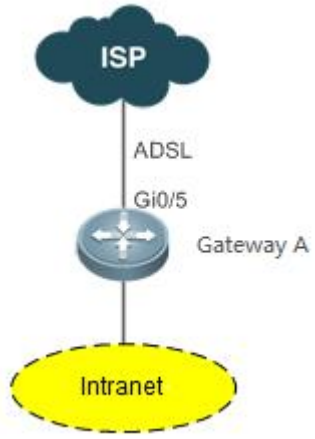
Configuration Example

The following configuration example describes configuration related to the PPPoE client only.

In the ADSL scenario, enable the PPPoE client function and access the Internet through an ADSL line.

Scenario

Figure 5- 5- 2



Configuration Steps	● Enable the PPPoE client function on the device, and add the interface Gi0/5 to the dialer pool.
A	A# configure terminal A(config)# interface GigabitEthernet 0/5 A(config-if)# pppoe enable A(config-if)# pppoe-client dial-pool-number 1 no-ddr A(config-if)# exit A(config)# interface dialer 1 A(config-if)# ip address negotiate A(config-if)# mtu 1488 A(config-if)# encapsulation ppp A(config-if)# ip nat outside A(config-if)# dialer pool 1 A(config-if)# dialer-group 1 A(config-if)# ppp chap hostname pppoe A(config-if)# ppp chap password pppoe A(config-if)# ppp pap sent-username pppoe password pppoe A(config-if)# exit A(config)# access-list 1 permit any A(config)# dialer-list 1 protocol ip permit A(config)# ip nat inside source list 1 interface dialer 1 A(config)# ip route 0.0.0.0 0.0.0.0 dialer 1 A(config)# end A#
Verification	Run the **show ip interface brief | in dialer** *1* command to check whether the dialer interface has acquired an IP address. Run the **show ip route** command to check whether a correct dialer interface route entry has been established. A# show ip interface brief | in dialer 1 dialer 1 49.1.1.127/32 YES UP A# show ip route

```
Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is 0.0.0.0 to network 0.0.0.0
S*    0.0.0.0/0 is directly connected, dialer 1
C     10.10.3.0/24 is directly connected, GigabitEthernet 0/0
C     10.10.3.1/32 is local host.
C     10.202.172.1/32 is directly connected, dialer 1
C     49.1.1.127/32 is local host.
```

Common Errors

- The negotiation fails because the user name or password is incorrect.
- Intranet hosts cannot access the Internet because NAT configuration is incorrect.
- Intranet hosts cannot access the Internet because route configuration is incorrect.

5.6 Monitoring

Clearing Various Information

If you run the **clear pppoe tunnel** command while the device is operating, packet forwarding will be interrupted due to tunnel clearance.

Function	Command
Clears statistics about the DDR dialer interface.	**clear dialer** [*interface-type interface-number*]
Clears the tunnel.	**clear pppoe tunnel**

Displaying the Running Status

Function	Command
Displays information about the DDR dialer.	**show dialer** [**interface** type number] [**maps**] [**pools**]
Displays PPPoE status information.	**show pppoe** { **ref** | **session** | **tunnel** }

Displaying Debugging Information

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Command	Function
debug dialer { **pkt** | **mlp**|**callback**|**event** }	Enables the DDR debugging switch.
debug ppp [**authentication** | **error** | **event** | **negotiation** | **packet**]	Enables the PPP negotiation debugging switch.

debug pppoe [**datas** | **errors** | **events** | **packets**]	Enables the PPPoE negotiation debugging switch.

6 Configuring PPPoE Server

6.1 Overview

The point-to-point protocol over Ethernet (PPPoE) enables an Ethernet host to connect to a remote access concentrator (AC) via a simple bridge. With PPPoE, the AC can control and charge each access user. Compared with traditional access modes, PPPoE features a low cost-performance ratio, and therefore it is applied in different fields, such as community network construction. At present, the popular broadband access mode ADSL is implemented using PPPoE.

PPPoE includes PPPoE client and PPPoE server. The PPPoE server is responsible for PPPoE connection requests, enabling users to access extranets. At present, home broadband connection is implemented by connecting the PPPoE client of a PC to the PPPoE server of an operator, realizing home Internet access.

Protocol Specifications

- RFC2516: A Method for Transmitting PPP Over Ethernet (PPPoE)

6.2 Applications

Application	Description
Configuring Local Authentication of PPPoE Server	Enables the PPPoE server on the AC and performs local authentication using a specified username. The IP address of a PPPoE client is allocated by the PPPoE server.
Configuring Remote Authentication of PPPoE Server	Enables the PPPoE server on the AC and performs remote authentication through AAA and RADIUS servers. The IP address of a PPPoE client is allocated by the PPPoE server.

6.2.1 Configuring Local Authentication of PPPoE Server

Scenario

A PPPoE client is connected to a wireless network through a wireless network card. Enable the PPPoE server on the AC and perform local authentication using a specified username. The IP address of the PPPoE client is allocated by the PPPoE server.

Figure 6- 1

Deployment

- Enable the PPPoE server on the AC to implement server function for PPPoE dialup.
- Configure a username and password on the AC to implement identity authentication for PPPoE dialup.
- Configure a local IP address pool on the AC to allocate IP addresses to hosts after PPPoE dialup is successful.
- Enable the PPPoE client on the host to implement Internet access by dialup.

6.2.2 Configuring Remote Authentication of PPPoE Server

Scenario

A PPPoE client is connected to a wireless network through a wireless network card. Enable the PPPoE server on the AC and perform remote authentication through AAA and RADIUS servers. The IP address of the PPPoE client is allocated by the PPPoE server.

Figure 6- 2

Deployment

- Enable the PPPoE server on the AC to implement server function for PPP dialup.
- Enable RADIUS authentication on the AC to implement RADIUS authentication for PPP users.
- Enable AAA authentication on the AC to implement AAA authentication for PPP users.
- Enable the PPPoE client on the host to implement Internet access by dialup.

6.3 Features

Basic Concepts

↘ AC-Cookie Tag

An AC-cookie tag is used by the PPPoE server to prevent DoS attacks. The PPPoE server can encapsulate the tag in PADO packets. After receiving the tag, the PPPoE client must encapsulate the tag in subsequent PADR packets. The tag value (TAG_VALUE) is binary data of any length and indicating any value, which cannot be interpreted by the PPPoE client.

Overview

Feature	Description
Local Authentication of PPPoE Server	Performs local authentication on the AC. The IP address of a PPPoE client is allocated from a local IP address pool.
Remote Authentication of PPPoE Server	Performs remote authentication through the AAA and RADIUS servers. The IP address of a PPPoE client is allocated by the RADIUS server.

6.3.1 Local Authentication of PPPoE Server

Local authentication is performed on the AC. The IP address of a PPPoE client is allocated from a local IP address pool.

Working Principle

PPPoE defines a model where multiple hosts connect to a remote AC (device that can complete such function is also referred to as a broadband access server) on a broadcast network (for example, Ethernet). In such model, the hosts must be capable of initializing their own PPP stack, so that the users can be charged and managed on the broadcast network based on the characteristics of PPP. To create and maintain point-to-point relationship between each host and the AC, a unique point-to-point session must be established between the host and AC.

PPPoE is composed of PPPoE Discovery Stage and PPPoE Session Stage. The session stage is equivalent to a PPP communication procedure, and the main difference lies in the PPPoE header in the PPP packets. Finally, packets will be encapsulated as Ethernet frames for transmission.

If a host expects to initiate a PPPoE session, the host will search for an AC on a broadcast network (in practice, cross-network access may exist. For example, an ATM network exists, and therefore PPPoEOA packets are generated). If there are multiple ACs on the network, the host will select an AC according to the service provided by the AC or user-defined configuration. After selecting an AC, the host establishes a PPPoE session with the AC and the AC will allocate a unique ID to the PPPoE session. During the session procedure, the host and AC (namely, the parties that create the point-to-point connection, which is logical and different from that of PPP) exchange packets over PPP. Finally, the host and AC transmit packets at the network layer through the point-to-point logical channel agreed on.

Related Configuration

Configuring Loopback Interface

No loopback interface is defined by default. With the loopback interface, the virtual template interface can borrow the IP address of the loopback interface and replicate the IP address to the virtual access interface to complete PPP negotiation.

Run the **interface loopback** xxx command to create a loopback interface. The IP address can be in the format of *A.B.C.D A.B.C.D.*

The loopback interface must be created and an IP address must be configured for the loopback interface. Otherwise, the virtual template interface cannot borrow the IP address of the loopback interface.

Configuring Username and Password

To complete PPP authentication, configure the username and password on the PPPoE server.

Run the **username** xxxx **password** xxxx command to configure the username and password.

If the PPPoE server uses AAA authentication, the username and password do not need to be configured.

Configuring Local IP Address Pool

To allocate IP addresses to clients during PPP negotiation, configure a local IP address pool on the PPPoE server.

Run the **ip local pool** *pool-name A.B.C.D A.B.C.D* command to configure a local IP address pool.

If the PPPoE server allocates IP address through the authentication server, the local IP address pool does not need to be configured.

Configuring Virtual Template

No virtual template available for the PPPoE server is configured on the broadband access server by default. After the PPPoE server is enabled, a virtual template interface must be created and relevant parameters must be configured for the interface, so that the virtual access interface can replicate configuration from the virtual template interface after a session is created.

Run the **interface virtual-template** number command to create a virtual template and enter the virtual template configuration mode.

In virtual template configuration mode, run the **ip unnumbered loopback** number command to borrow the IP address of the loopback interface.

In virtual template configuration mode, run the **ppp authentication {chap | pap } [**list-name**]** command to configure the authentication mode as CHAP or PAP. PPPoE supports CHAP and PAP authentication modes and can apply local or remote authentication according to the network topology. If remote authentication is used, associate the virtual template with the enabled user authentication list. For details, refer to the *Configuring AAA.*

In virtual template configuration mode, run the **peer default ip address pool** local command to allocate an IP address in the local IP address pool to the PPPoE client.

A virtual template must be configured for the PPPoE server.

Configuring bba-group

To complete the functions on the PPPoE server, the interface with the PPPoE server enabled must be associated with the bba-group PPPoE dialup group. In the bba-group PPPoE dialup group, set the PPPoE server, connection limit, and virtual template.

Run the **bba-group pppoe** pppoe_group command to configure the bba-group.

Mandatory. In bba-group configuration mode, run the **virtual-template** number command to associate the virtual template.

Optional. In bba-group configuration mode, run the **ac-cookie enable** command to enable the AC cookie function.

Optional. In bba-group configuration mode, run the **sessions local-mac limit** count command to configure the maximum number of sessions that a PPPoE client can initiate using one MAC address.

Optional. In bba-group configuration mode, run the **sessions per-mac limit** count command to configure the maximum number of sessions that a PPPoE server can process using one MAC address.

Optional. In bba-group configuration mode, run the **sessions max limit** count command to configure the maximum number of sessions that the AC can process.

Enabling PPPoE Server on Interface

This section describes the general switch of the PPPoE server.

In interface configuration mode, run the **pppoe-server enable group** pppoe_group command to enable the PPPoE server and associate the bba-group.

The PPPoE server is disabled on an interface by default.

6.3.2 Remote Authentication of PPPoE Server

Remote authentication is performed in conjunction with the AAA and RADIUS servers. The IP address of a PPPoE client is allocated by the RADIUS server.

Working Principle

The working principle of remote authentication is similar to that of local authentication. The difference lies in that the authentication data is sent by the PPPoE server to the AAA and RADIUS servers for joint authentication. Compared with local authentication, remote authentication is implemented based on AAA, and therefore the username and password do not need to be configured.

Related Configuration

The working procedure of remote authentication is similar to that of local authentication. Except the username and password, other configurations are required.

Associating Virtual Template with PPP User Authentication List

In global configuration mode, run the **ppp authentication {chap | pap | ms-chap | ms-chap-v2}** *list-name* command to associate the virtual template with a PPP user authentication list. For details, refer to the *PPP-SCG*.

Enabling AAA

In global configuration mode, run the **aaa authentication ppp** *list-name* **group radius** command to enable RADIUS authentication for the PPP user list.

In global configuration mode, run the **aaa new-model** command to enable AAA authentication.

For details, refer to the *AAA-SCG*.

Configuring RADIUS Authentication

In global configuration mode, run the **radius-server host** *ipv4-address* command to configure a RADIUS server.

In global configuration mode, run the **radius-server key** [0 | 7] *text-string* command to configure a password for communicating with the RADIUS server.

For details, refer to the *AAA-SCG*.

6.4 Configuration

Configuration	Description and Command

Configuring Local Authentication of PPPoE Server	(Mandatory) It is used to configure local authentication of PPPoE server. If remote authentication is selected, except the username and password, other configurations are required.	
	interface loopback *number*	Configures a loopback interface.
	ip address *A.B.C.D A.B.C.D*	Configures an IP address of the loopback interface.
	username *username* **password** *password*	Configures the username and password. If the PPPoE server uses AAA authentication, the username and password do not need to be configured.
	ip local pool *pool-name A.B.C.D A.B.C.D*	Configures a local IP address pool.
	interface virtual-template *number*	Configures a virtual template.
	ip unnumber loopback *number*	Borrows the IP address of the loopback interface. The configuration is performed in virtual template interface configuration mode.
	ppp authentication {chap | pap | ms-chap | ms-chap-v2 }	Configures the authentication mode as CHAP or PAP. PPPoE supports CHAP and PAP authentication modes and can apply local or remote authentication according to the network topology. If remote authentication is used, associate the virtual template with the enabled user authentication list. For details, refer to the *AAA-SCG*. The configuration is performed in virtual template interface configuration mode.
	peer default ip address pool *pool-name*	Configures the name of the IP address pool. The configuration is performed in virtual template interface configuration mode.
	pppoe server enable	Enables the PPPoE server function.
	bba-group pppoe *pppoe_group*	Configures a bba-group.
	virtual-template *number*	Associates the bba-group with the virtual template interface.
	pppoe-server enable group *pppoe_group*	Enables the PPPoE server on the interface that connects to a PPPoE client and associates the PPPoE server with the bba-group.
Configuring Remote Authentication of PPPoE Server	(Optional) It is used to configure remote authentication of PPPoE server.	
	aaa new-model	Enables AAA.
	aaa authentication ppp *list-name* **group radius**	Enables RADIUS authentication for the PPP user list.
	ppp authentication {chap | pap } [*list-name***]**	Associates the virtual template with a PPP user authentication list.
	radius-server host *ipv4-address*	Configures a RADIUS server.

	radius-server key [0 | 7] *text-string*	Configures a password for RADIUS authentication.

6.4.1 Configuring Local Authentication of PPPoE Server

Configuration Effect

Perform local authentication on a PPPoE client using a specified username. The IP address of the PPPoE client is allocated by the PPPoE server.

Notes

N/A

Configuration Steps

Configuring Loopback Interface

- Mandatory.
- Users can configure a L3 interface as well, but a loopback interface will be always up after an IP address is configured for it.

Configuring Username and Password

- Configure the username and password if local authentication is used. The configuration is not required if AAA authentication is used.

Configuring Local IP Address Pool

- Mandatory.
- Generally, set the range of an IP address pool to be consistent with the network segment of the loopback interface to save route configuration.

Configuring Virtual Template

- Mandatory.
- Associate the virtual template with the enabled user authentication list if remote authentication is used. For details, refer to the *Configuring AAA*.
- In bba-group configuration mode or global configuration mode, configure the virtual template interface.

Enabling PPPoE Server

- Mandatory.

Configuring bba-group

- Mandatory. Associate the bba-group with the virtual template interface.

Enabling PPPoE Server and Associating with bba-group

- Mandatory. Associate the PPPoE server with the bba-group.
- Configure the bba-group in interface configuration mode, for example, on the interface of VLAN 1.

Verification

Verify that the Internet can be accessed using a PPPoE client by dialup.

Related Commands

Creating Loopback Interface

Command	**interface loopback** *number*
Parameter Description	*number*: Indicates the ID of a new loopback interface.

Command Mode	Global configuration mode
Usage Guide	N/A

Configuring IP Address of Loopback Interface

Command	**ip address** *A.B.C.D A.B.C.D*
Parameter Description	*A.B.C.D A.B.C.D*: Indicates an IP address.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring Username and Password

Command	**username** *username* **password** *password*
Parameter Description	*username*: Indicates a username. *password*: Indicates a password.
Command Mode	Global configuration mode
Usage Guide	If the PPPoE server uses AAA authentication, the username and password do not need to be configured.

Creating Local IP Address Pool

Command	**ip local pool** *pool-name A.B.C.D A.B.C.D*
Parameter Description	*pool-name*: Indicates an IP address pool. *A.B.C.D A.B.C.D*: Indicates the range of IP addresses.
Command Mode	Global configuration mode
Usage Guide	N/A

Creating Virtual Template

Command	**interface virtual-template** *number*
Parameter Description	*number*: Indicates the ID of a new virtual template.
Command Mode	Global configuration mode
Usage Guide	N/A

Borrowing IP Address of Loopback Interface

Command	**ip unnumbered loopback** *number*
Parameter Description	*number*: Indicates the ID of a new loopback interface.
Command Mode	Virtual template configuration mode
Usage Guide	N/A

Configuring Authentication Mode as CHAP or PAP

Command	**ppp authentication {chap | pap }** [*list-name*]
Parameter Description	*list-name*: Indicates an authentication list. Generally, this list is used during AAA authentication.

Command Mode	Virtual template configuration mode
Usage Guide	PPPoE supports CHAP and PAP authentication modes and can apply local or remote authentication according to the network topology. If remote authentication is used, associate the virtual template with the enabled user authentication list. For details, refer to the *AAA-SCG*.

Configuring Name of IP Address Pool

Command	**peer default ip address pool** *pool-name*
Parameter Description	*pool-name*: Indicates an IP address pool.
Command Mode	Virtual template configuration mode
Usage Guide	N/A

Creating bba-group

Command	**bba-group pppoe** *group-name*
Parameter Description	*group-name*: Indicates a bba-group.
Command Mode	Global configuration mode
Usage Guide	N/A

Associating bba-group with Virtual Template

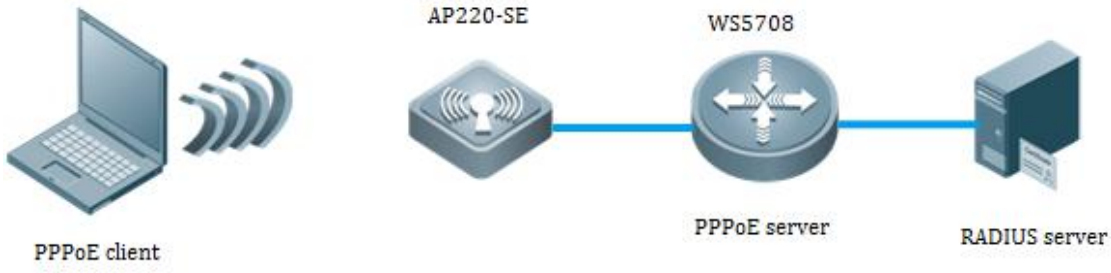
Command	**virtual-template** *number*
Parameter Description	*number*: Indicates the ID of a virtual template.
Command Mode	bba-group mode
Usage Guide	N/A

Enabling PPPoE Server

Command	**pppoe-server enable group** *bba-group*
Parameter Description	*bba-group*: Indicates the name of a virtual bba-group.
Command Mode	Interface configuration mode
Usage Guide	Enable the PPPoE server on the interface that connects to a PPPoE client and associate the PPPoE server with the bba-group.

Configuration Example

Configuring Local Authentication of PPPoE Server

Scenario Figure 6-3	
Configuration Steps	● Configure local authentication on the PPPoE server. ● Connect a PPPoE client to the AC using a wireless network card by PPPoE.
PPPoE Server	# Configuring a username and a password. FS#conf FS(config)#username FS password FS FS(config)#end FS# # Configuring a local IP address pool. FS#conf FS(config)#ip local pool pppoe 1.2.3.4 1.2.3.254 FS(config)#end FS# # Note: The following configuration items do not impose requirements on the configuration order. # Enabling the PPPoE server. FS#conf FS(config)#pppoe-server enable # Configuring a bba-group. FS#conf FS(config)#bba-group pppoe pppoe1 FS(config-bba-group)#virtual-template 2 FS(config-bba-group)#exit FS(config)#end FS# # Configuring a loopback interface. FS#conf FS(config)#int loopback 1 FS(config-if-Loopback 1)#ip address 1.2.3.1 24 FS(config-if-Loopback 1)#end FS#

	# Configuring a virtual template. FS#conf FS(config)#int virtual-template 2 FS(config-if-Virtual-Template 2)#ip unnumbered loopback 1 FS(config-if-Virtual-Template 2)#ppp authentication pap chap FS(config-if-Virtual-Template 2)#peer default ip address pool pppoe FS(config-if-Virtual-Template 2)#end FS# # Configuring a VLAN and enabling the PPPoE server. FS#conf FS(config)#vlan 1 FS(config-vlan)#exit FS(config)#int vlan 1 FS(config-if-VLAN 1)#pppoe-server enable group pppoe1 FS(config-if-VLAN 1)#end FS# FS#
PPPoE Client	Ensure that the PC has been installed with a wireless network card drive of corresponding model and search for the SSID configured on the PPPoE server. Configure the SSID as a preferred network, as shown in the following figure: Choose **My Network Places** > **View Network Connection**s and create a new connection. Click **Next** and select **Connect to the Internet (C)**. Select **Manually Set My Connection (M)**. Select **Use Specified Username and Password for Broadband Connection (U)**. Enter the ISP name FS_1. Enter the username and password provided by the PPPoE server. In this example, the username and password are both FS. B(config)# ip pim bsr-candidate loopback 0
Verification	● Run the **show pppoe session** command on the PPPoE server to display the connection status. ● Connect to the Internet using a PPPoE client by dialup.
PPPoE server	FS#show pppoe-server session # The information about the PPPoE server is displayed as follows:

	Sid State intf external-vid inner-vid Peer LocalMAC RemoteMAC online time 20 STATE_SESSION virtual-access 5091 1 0 7.7.7.2 00:D0:F8:22:12:81 08:FB:0A:B0:48:AF 0 day(s) 15:16:31 PPPOE Server current sessions count : 1
PPPoE client	The PC is successfully connected to the Internet.

6.4.2 Configuring Remote Authentication of PPPoE Server

Configuration Effect

- Complete remote authentication using a PPPoE client in conjunction with the AAA and RADIUS servers.

Notes

- Except the username and password, other basic information of the PPPoE server must be configured.

Configuration Steps

Enabling AAA

- Mandatory.
- Enable the AAA function in global configuration mode.

Enabling RADIUS Authentication for PPP User List

- Mandatory.

Associating Virtual Template with PPP User Authentication List

- Mandatory.
- Specify an authentication mode or list.
- Associate the virtual template with the PPP user authentication list in virtual template interface configuration mode.

Configuring RADIUS Authentication

- Mandatory.
- Configure the IP address and password of the RADIUS server.

Verification

Connect to the Internet using a PPPoE client by dialup.

Related Commands

Enabling AAA

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling RADIUS Authentication for PPP User List

Command	**aaa authentication ppp** *list-name* **group radius**
Parameter Description	*list-name*: Indicates a PPP user authentication list.

Command Mode	Global configuration mode
Usage Guide	N/A

Associating Virtual Template with PPP User Authentication List

Command	**ppp authentication {chap | pap }** *list-name*
Parameter Description	**chap**: Indicates the authentication mode CHAP. **pap**: Indicates the authentication mode PAP. *list-name*: Indicates a PPP user authentication list.
Command Mode	Virtual template configuration mode
Usage Guide	N/A

Configuring RADIUS Server

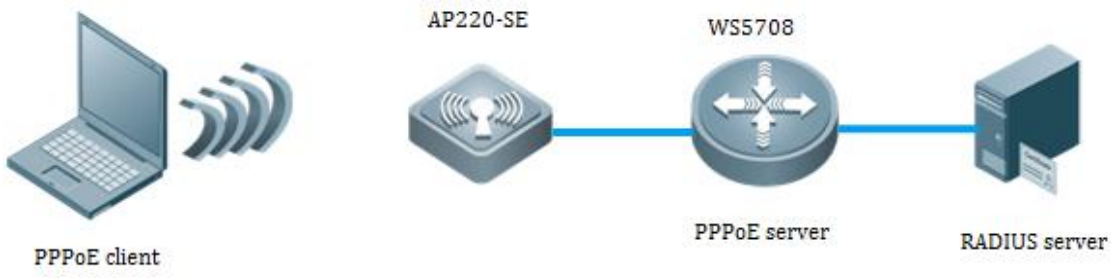
Command	**radius-server host** *ipv4-address*
Parameter Description	*ipv4-address*: Indicates the IP address of a RADIUS server.
Command Mode	Global configuration mode
Usage Guide	To implement AAA security service, define one or multiple RADIUS servers by running the **radius-server host** command.

Configuring Password for Communicating with RADIUS Server

Command	**radius-server key** [0 | 7] *text-string*
Parameter Description	*text-string*: Indicates text of a password. 0 | 7: Indicates an encryption type of the password. 0 indicates no encryption, and 7 indicates simple encryption.
Command Mode	Global configuration mode
Usage Guide	The password lays a foundation for communication between the AC and RADIUS server. To ensure the communication, configure the same password on the AC and RADIUS server.

Configuration Example

Configuring Remote Authentication of PPPoE Server

Scenario Figure 6-4	
Configuration Steps	● Configure basic functions of the PPPoE server. ● Configure AAA and RADIUS servers.
PPPoE server	# Note: The following configuration items do not impose requirements on the configuration order.

```
# Enabling AAA.
FS#conf
FS(config)#aaa new-model
FS(config)#exit
FS#
# Enabling RADIUS authentication for the PPP user list.
FS#conf
FS(config)#aaa authentication ppp default group radius
FS(config)#exit
FS#

# Configuring the IP address and password of the RADIUS server.
FS#conf
FS(config)#radius-server host 192.168.23.71
FS(config)#radius-server key FS
FS(config)#end
FS#

# Configuring a local IP address pool.
FS#conf
FS(config)#ip local pool pppoe 1.2.3.4 1.2.3.254
FS(config)#end
FS#

# Enabling the PPPoE server.
FS#conf
FS(config)#pppoe-server enable

# Configuring a bba-group.
FS#conf
FS(config)#bba-group pppoe pppoe1
FS(config-bba-group)#virtual-template 2
FS(config-bba-group)#exit
FS(config)#end
FS#

# Configuring a loopback interface.
FS#conf
FS(config)#int loopback 1
FS(config-if-Loopback 1)#ip address 1.2.3.1 24
FS(config-if-Loopback 1)#end
FS#

# Configuring a virtual template.
```

	FS#conf FS(config)#int virtual-template 2 FS(config-if-Virtual-Template 2)#ip unnumbered loopback 1 FS(config-if-Virtual-Template 2)#ppp authentication pap chap FS(config-if-Virtual-Template 2)#peer default ip address pool pppoe FS(config-if-Virtual-Template 2)#end FS# # Configuring a VLAN and enabling the PPPoE server. FS#conf FS(config)#vlan 1 FS(config-vlan)#exit FS(config)#int vlan 1 FS(config-if-VLAN 1)#pppoe-server enable group pppoe1 FS(config-if-VLAN 1)#end FS# FS#
PPPoE client	For details, refer to the configurations for local authentication.
Verification	● Run the **show pppoe-server session** command on the PPPoE server to display the connection status. ● Connect to the Internet using a PPPoE client by dialup.
PPPoE server	FS#show pppoe-server session # The information about the PPPoE server is displayed as follows: Sid State intf external-vid inner-vid Peer LocalMAC RemoteMAC online time 20 STATE_SESSION virtual-access 5091 1 0 7.7.7.2 00:D0:F8:22:12:81 08:FB:0A:B0:48:AF 0 day(s) 15:16:31 PPPOE Server current sessions count : 1
PPPoE client	The PC is successfully connected to the Internet.

6.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears all PPPoE tunnels of the system.	**clear pppoe-server tunnel**
Clears the PPPoE tunnels with specified session IDs.	**clear pppoe-server tunnel session-id** *id*

Displaying

Description	Command

Displays all session information and forwarding plane information of the system. Note: The tunnel information is consistent with the session information.	**show pppoe-server { tunnel | session | ref }**

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs the switch of PPPoE session packets.	**debug pppoe datas**
Debugs the output switch of PPPoE exception information.	**debug pppoe errors**
Debugs the switch of PPPoE negotiation.	**debug pppoe events**
Debugs the switch of PPPoE negotiation packets.	**debug pppoe packets**
Debugs the PPP LCP and IPCP negotiation switches.	**debug ppp negotiation**
Debugs the negotiation switch of PPP authentication.	**debug ppp authentication**
Debugs the error information switch throughout the PPP negotiation stage.	**debug ppp error**

7 Configuring Aggregated Port

7.1 Overview

An aggregated port (AP) is used to bundle multiple physical links into one logical link to increase the link bandwidth and improve connection reliability.

An AP port supports load balancing, namely, distributes load evenly among member links. Besides, an AP port realizes link backup. When a member link of the AP port is disconnected, the load carried by the link is automatically allocated to other functional member links. A member link does not forward broadcast or multicast packets to other member links.

For example, the link between two devices supports a maximum bandwidth of 1,000 Mbps. When the service traffic carried by the link exceeds 1,000 Mbps, the traffic in excess will be discarded. Port aggregation can be used to solve the problem. For example, you can connect the two devices with network cables and combine multiple links to form a logical link capable of multiples of 1,000 Mbps.

For example, there are two devices connected by a network cable. When the link between the two ports of the devices is disconnected, the services carried by the link will be interrupted. After the connected ports are aggregated, the services will not be affected as long as one link remains connected.

Protocols and Standards

- IEEE 802.3ad

7.2 Applications

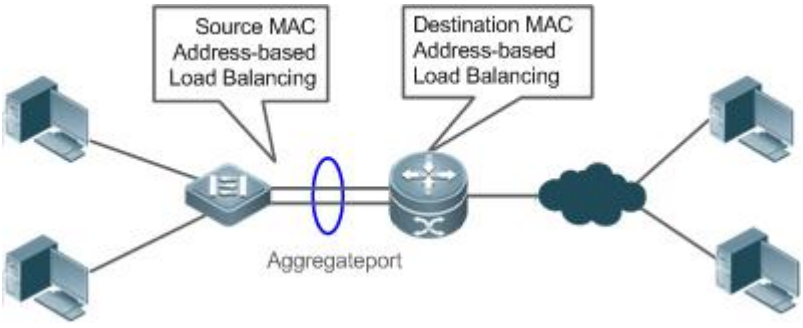
Applications	Description
AP Link Aggregation and Load Balancing	A large number of packets are transmitted between an aggregation device and a core device, which requires a greater bandwidth. To meet this requirement, you can bundle the physical links between the devices into one logical link to increase the link bandwidth, and configure a proper load balancing algorithm to distribute the work load evenly to each physical link, thus improving bandwidth utilization.

7.2.1 AP Link Aggregation and Load Balancing

Scenario

In Figure 6-1, the switch communicates with the router through an AP port. All the devices on the intranet (such as the two PCs on the left) use the router as a gateway. All the devices on the extranet (such as the two PCs on the right) send packets to the internet devices through the router, with the gateway's MAC address as its source MAC address. To distribute the load between the router and other hosts to other links, configure destination MAC address-based load balancing. On the switch, configure source MAC address-based load balancing.

Figure 6-1 AP Link Aggregation and Load Balancing



Deployment

- Configure the directly connected ports between the switch and router as a static AP port or a Link Aggregation Control Protocol AP port.
- On the switch, configure a source MAC address-based load balancing algorithm.
- On the router, configure a destination MAC address-based load balancing algorithm.

7.3 Features

Basic Concepts

Static AP

The static AP mode is an aggregation mode in which physical ports are directly added to an AP aggregation group through manual configuration to allow the physical ports to forward packets when the ports are proper in link state and protocol state.

An AP port in static AP mode is called a static AP, and its member ports are called static AP member ports.

AP Member Port State

There are two kinds of AP member port state available:

- When a member port is Down, the port cannot forward packets. The Down state is displayed.
- When a member port is Up and the link protocol is ready, the port can forward packets. The Up state is displayed.

Overview

Overview	Description
Link Aggregation	Aggregates physical links statically or dynamically to realize bandwidth extension and link backup.
Load Balancing	Balances the load within an aggregation group flexibly by using different load balancing methods.

7.3.1 Link Aggregation

Working Principle

- Static AP

The static AP configuration is simple. Run a command to add the specified physical port to the AP port. After joining the aggregation group, a member port can receive and transmit data and participate in load balancing within the group.

7.3.2 Load Balancing

Working Principle

AP ports segregate packet flows by using load balancing algorithms based on packet features, such as the source and destination MAC addresses, source and destination IP addresses, and Layer-4 source and destination port numbers. The packet flow with the consistent feature is transmitted by one member link, and different packet flows are evenly distributed to member links. For example, in source MAC address-based load balancing, packets are distributed to the member links based on the source MAC addresses of the packets. Packets with different source MAC addresses are evenly distributed to member links. Packets with the identical source MAC address are forwarded by one member link.

Currently, there are several AP load balancing modes as follows:

- Source MAC address or destination MAC address
- Source MAC address + destination MAC address
- Source IP address or destination IP address
- Source IP address + destination IP address

- Layer-4 source port number or Layer-4 destination port number
- Layer-4 source port number + Layer-4 destination port number
- Source IP address + Layer-4 source port number
- Source IP address + Layer-4 destination port number
- Destination IP address + Layer-4 source port number
- Destination IP address + Layer-4 destination port number
- Source IP address + Layer-4 source port number + Layer-4 destination port number
- Destination IP address + Layer-4 source port number + Layer-4 destination port number
- Source IP address + destination IP address + Layer-4 source port number
- Source IP address + destination IP address + Layer-4 destination port number
- Source IP address + destination IP address + Layer-4 source port number + Layer-4 destination port number
- Panel port for incoming packets

Load balancing based on IP addresses or port numbers is applicable only to Layer-3 packets. When a device enabled with this load balancing method receives Layer-2 packets, it automatically switches to the default load balancing method.

All the load balancing methods use a load algorithm (hash algorithm) to calculate the member links based on the input parameters of the methods. The input parameters include the source MAC address, destination MAC address, source MAC address + destination MAC address, source IP address, destination IP address, source IP address + destination IP addresses, source IP address + destination IP address + Layer-4 port number and so on. The algorithm ensures that packets with different input parameters are evenly distributed to member links. It does not indicate that these packets are always distributed to different member links. For example, in IP address-based load balancing, two packets with different source and destination IP addresses may be distributed to the same member link through calculation.

Different products may support different load balancing algorithms.

7.3.3 Wireless AP Aggregated Port

Working Principle

If the wireless traffic exceeds gigabit, a single wired port cannot meet the requirements. In this case, an aggregated port needs to be used for load balancing and bandwidth increasing. Wireless APs adopts the dual uplink deployment mode. If a network cable is disconnected, the other cable can continue to work, ensuring link backup. Aggregated port configuration of wireless APs is delivered by the AC or aggregated ports are configured independently on the APs. If wireless APs work in fit AP mode, aggregated port configuration is delivered by the AC. If wireless APs work in fat AP mode, aggregated ports are configured on the AP console over serial ports.

7.4 Limitations

EG3000XE and EG3000UE support WAN port aggregation; EG2000CE does not support WAN port aggregation.

7.5 Configuration

Configuration	Description and Command	
Configuring Static AP Ports	(Mandatory) It is used to configure link aggregation manually.	
	interface aggregateport	Creates an Ethernet AP port.
Enabling LinkTrap	(Optional) It is used to enable LinkTrap.	
	aggregateport member linktrap	Enables LinkTrap t for AP member ports.

Configuration	Description and Command	
Configuring a Load Balancing Mode	(Optional) It is used to configure a load balancing mode for an aggregated link.	
	aggregateport load-balance	Configures a load balancing algorithm for an AP port or AP member ports.
Configuring Aggregated Port Configuration Delivery from the AC	**ap-interface wireport** *portnumber* **port-group** *apnumber*	Configures aggregated port configuration delivery from the AC.

7.5.1 Configuring Static AP Ports

Configuration Effect

- Configure multiple physical ports as AP member ports to realize link aggregation.
- The bandwidth of the aggregation link is equal to the sum of the member link bandwidths.
- When a member link of the AP port is disconnected, the load carried by the link is automatically allocated to other functional member links.

Notes

- Only physical ports can be added to an AP port.
- The ports of different media types or port modes cannot be added to the same AP port.
- Layer-2 ports can be added to only a Layer-2 AP port, and Layer-3 ports can be added to only a Layer-3 AP port. The Layer-2/3 attributes of an AP port that contains member ports cannot be modified.
- After a port is added to an AP port, the attributes of the port are replaced by those of the AP port.
- After a port is removed from an AP port, the attributes of the port are restored.

After a port is added to an AP port, the attributes of the port are consistent with those of the AP port. Therefore, do not perform configuration on the AP member ports or apply configuration to a specific AP member port. However, some configurations (the **shutdown** and **no shutdown** commands) can be configured on AP member ports. When you use AP member ports, check whether the function that you want to configure can take effect on a specific AP member port, and perform this configuration properly.

Configuration Steps

Creating an Ethernet AP Port

- Mandatory.
- Perform this configuration on an AP-enabled device.

Command	**interface aggregateport** *ap-number*
Parameter Description	*ap-number*: Indicates the number of an AP port.
Defaults	By default, no AP port is created.
Command Mode	Global configuration mode
Usage Guide	To create an Ethernet AP port, run **interfaces aggregateport** in global configuration mode. To delete the specified Ethernet AP port, run **no interfaces aggregateport** *ap-number* in global configuration mode.

Run **port-group** to add a physical port to a static AP port in interface configuration mode. If the AP port does not exist, it will be created automatically.

Configuring Static AP Member Ports

- Mandatory.
- Perform this configuration on AP-enabled devices.

Command	**port-group** *ap-number*
Parameter Description	**port-group** *ap-number*: Indicates the number of an AP port.
Defaults	By default, no ports are added to any static AP port.
Command Mode	Interface configuration mode of the specified Ethernet port
Usage Guide	To add member ports to an AP port, run **port-group** in interface configuration mode. To remove member ports from an AP port, run **no port-group** in interface configuration mode.

The static AP member ports configured on the devices at both ends of a link must be consistent.

After a member port exits the AP port, the default settings of the member port are restored. Different functions deal with the default settings of the member ports differently. It is recommended that you check and confirm the port settings after a member port exits an AP port.

After a member port exits an AP port, the port is disabled by using the **shutdown** command to avoid loops. After you confirm that the topology is normal, run **no shutdown** in interface configuration mode to enable the port again.

Creating an Ethernet AP Subinterface

- Optional.
- On a device that supports subinterface configuration, run **interface aggregateport** *sub-ap-number* to create a subinterface.
- Perform this configuration on AP-enabled devices that support Layer-2 and Layer-3 features, such as Layer-3 switches.

Command	**interface aggregateport** *sub-ap-number*
Parameter Description	*sub-ap-number*: Indicates the number of an AP subinterface.
Defaults	By default, no subinterfaces are created.
Command Mode	Interface configuration mode of the specified AP port
Usage Guide	You need to convert the master port of the AP port to a Layer-3 port before creating a subinterface.

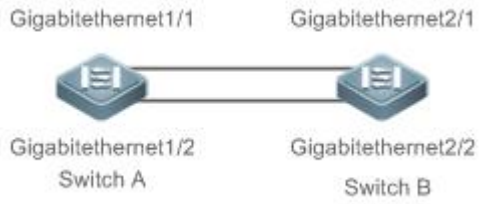
Verification

- Run **show running** to display the configuration.
- Run **show aggregateport summary** to display the AP configuration.

Command	**show aggregateport** *aggregate-port-number* [**load-balance** | **summary**]
Parameter Description	*aggregate-port-number*: Indicates the number of an AP port. **load-balance**: Displays the load balancing algorithm. **summary**: Displays the summary of each link.
Command Mode	Any mode
Usage Guide	The information on all AP ports is displayed if you do not specify the AP port number.
	FS# show aggregateport 1 summary AggregatePort MaxPorts SwitchPort Mode Load balance Ports ---------- ---------- ---------- ------ ---------- ---------- **Ag1** 8 Enabled ACCESS **dst-mac** **Gi0/2**

Configuration Example

Configuring an Ethernet Static AP Port

Scenario **Figure 6-2**	
Configuration Steps	● Add the GigabitEthernet 1/1 and GigabitEthernet 1/2 ports on Switch A to static AP port 3. ● Add the GigabitEthernet 2/1 and GigabitEthernet 2/2 ports on Switch B to static AP port 3.
Switch A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3
Switch B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 2/1-2 SwitchB(config-if-range)# port-group 3
Verification	● Run **show aggregateport summary** to check whether AP port 3 contains member ports GigabitEthernet 1/1 and GigabitEthernet 1/2.
Switch A	SwitchA# show aggregateport summary AggregatePort MaxPorts SwitchPort Mode Ports ---------- -------- ---------- ------ ---------- **Ag3** 8 Enabled ACCESS **Gi1/1,Gi1/2**
Switch B	SwitchB# show aggregateport summary AggregatePort MaxPorts SwitchPort Mode Ports ---------- -------- ---------- ------ ---------- **Ag3** 8 Enabled ACCESS **Gi2/1,Gi2/2**

7.5.2 Enabling LinkTrap

Configuration Effect

Enable the system with LinkTrap to send LinkTrap messages when aggregation links are changed.

Configuration Steps

Enabling LinkTrap for AP Member Ports

- Optional.
- By default, LinkTrap is disabled for AP member ports.
- Perform this configuration on AP-enabled devices.

Command	**aggregateport member linktrap**
Parameter Description	N/A
Defaults	By default, LinkTrap is disabled for AP member ports.
Command Mode	Global configuration mode
Usage Guide	Use this command in global configuration mode to enable LinkTrap for all AP member ports. By default, LinkTrap messages are not sent when the link state of AP member ports is changed. To disable LinkTrap for all AP member

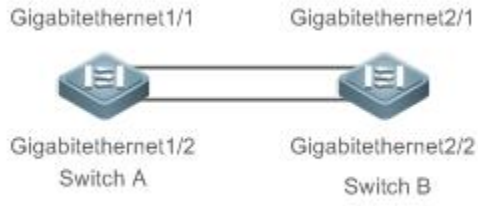
	ports, run **no aggregateport member linktrap** in global configuration mode.

Verification

- Run **show running** to display the configuration.
- After LinkTrap is enabled, you can monitor this feature on AP ports or their member ports by using the MIB software.

Configuration Example

Enabling LinkTrap for AP Member Ports

Scenario **Figure 6-3**	
Configuration Steps	● Add the GigabitEthernet 1/1 and GigabitEthernet 1/2 ports on Switch A to static AP port 3. ● Add the GigabitEthernet 2/1 and GigabitEthernet 2/2 ports on Switch B to static AP port 3. ● On Switch A, disable LinkTrap for AP port 3 and enable LinkTrap for its member ports. ● On Switch B, disable LinkTrap for AP port 3 and enable LinkTrap its AP member ports.
Switch A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3 SwitchA(config-if-range)# exit SwitchA(config)# aggregateport member linktrap
Switch B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 2/1-2 SwitchB(config-if-range)# port-group 3 SwitchB(config-if-range)# exit SwitchB(config)# aggregateport member linktrap
Verification	● Run **show running** to check whether LinkTrap is enabled for AP port 3 and its member ports.
Switch A	SwitchA# show run | include AggregatePort 3 Building configuration... Current configuration: 54 bytes interface AggregatePort 3 no snmp trap link-status SwitchA# show run | include AggregatePort aggregateport member linktrap
Switch B	SwitchB# show run | include AggregatePort 3 Building configuration... Current configuration: 54 bytes interface AggregatePort 3 no snmp trap link-status SwitchB# show run | include AggregatePort aggregateport member linktrap

7.5.3 Configuring a Load Balancing Mode

Configuration Effect

The system distributes incoming packets among member links by using the specified load balancing algorithm. The packet flow with the consistent feature is transmitted by one member link, whereas different packet flows are evenly distributed to various links. A device enabled with enhanced load balancing first determines the type of packets to be transmitted and performs load balancing based on the specified fields in the packets. For example, the AP port performs source IP-based load balancing on the packets containing an ever-changing source IPv4 address.

Notes

- N/A

Configuration Steps

Configuring the Global Load Balancing Algorithm of an AP port

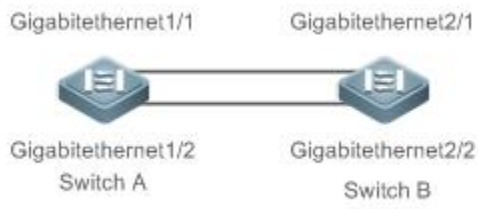
- (Optional) Perform this configuration when you need to optimize load balancing.
- Perform this configuration on AP-enabled devices.

Command	**aggregateport load-balance** { **dst-mac** | **src-mac** | **src-dst-mac** | **dst-ip** | **src-ip** | **src-dst-ip** | **src-dst-ip-l4port** | **src- l4port** | **dst-l4port** | **src-dst-l4port** | **src-ip-src-l4port** | **src-ip-dst-l4port** | **dst-ip-src-l4port** | **dst-ip-dst-l4port** | **src-ip-src-dst-l4port** | **dst-ip-src-dst-l4port** | **src-dst-ip-src-l4port** | **src-dst-ip-dst-l4port** }
Parameter Description	**dst-mac**: Indicates that load is distributed based on the destination MAC addresses of incoming packets. **src-mac**: Indicates that load is distributed based on the source MAC addresses of incoming packets. **src-dst-ip**: Indicates that load is distributed based on source and destination IP addresses of incoming packets. **dst-ip**: Indicates that load is distributed based on the destination IP addresses of incoming packets. **src-ip**: Indicates that load is distributed based on the source IP addresses of incoming packets. **src-dst-mac**: Indicates that load is distributed based on source and destination MAC addresses of incoming packets. **src-dst-ip-l4port**: Indicates that load is distributed based on source IP and destination IP addresses as well as Layer-4 source and destination port numbers. **src- l4port**: Indicates that load is distributed based on Layer-4 source port numbers. **dst- l4port**: Indicates that load is distributed based on Layer-4 destination port numbers. **src-dst-l4port**: Indicates that load is distributed based on Layer-4 source and destination port numbers. **src-ip-src-l4port**: Indicates that load is distributed based on source IP addresses and Layer-4 source port numbers. **src-ip-dst-l4port**: Indicates that load is distributed based on source IP addresses and Layer-4 destination port numbers. **dst-ip-src-l4port**: Indicates that load is distributed based on destination IP addresses and Layer-4 source port numbers. **dst-ip-dst-l4port**: Indicates that load is distributed based on destination IP addresses and Layer-4 destination port numbers. **src-ip-src-dst-l4port:** Indicates that load is distributed based on source IP addresses as well as Layer-4 source and destination port numbers. **dst-ip-src-dst-l4port**: Indicates that load is distributed based on destination IP addresses as well as Layer-4 source and destination port numbers. **src-dst-ip-src-l4port**: Indicates that load is distributed based on source and destination IP addresses as well as Layer-4 source port numbers. **src-dst-ip-dst-l4port**: Indicates that load is distributed based on source and destination IP addresses as well as Layer-4 destination port numbers.

Defaults	Load balancing can be based on source and destination MAC addresses, source and destination IP addresses (applicable to gateways), or the profile of enhanced load balancing.
Command Mode	Global configuration mode
Usage Guide	To restore the default settings, run **no aggregateport load-balance** in global configuration mode. You can run **aggregateport load-balance** in interface configuration mode of an AP port on devices that support load balancing configuration on a specific AP port. The configuration in interface configuration mode prevails. To disable the load balancing algorithm, run **no aggregateport load-balance** in interface configuration mode of the AP port. After that, the load balancing algorithm configured in global configuration mode takes effect. You can run **aggregateport load-balance** in interface configuration mode of an AP port on devices that support load balancing configuration on a specific AP port.

Configuration Example

Configuring a Load Balancing Mode

Scenario **Figure 6-4**	
Configuration Steps	● Add the GigabitEthernet 1/1 and GigabitEthernet 1/2 ports on Switch A to static AP port 3. ● Add the GigabitEthernet 2/1 and GigabitEthernet 2/2 ports on Switch B to static AP port 3. ● On Switch A, configure source MAC address-based load balancing for AP port 3 in global configuration mode. ● On Switch B, configure destination MAC address-based load balancing for AP port 3 in global configuration mode.
Switch A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3 SwitchA(config-if-range)# exit SwitchA(config)# aggregateport load-balance src-mac
Switch B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 2/1-2 SwitchB(config-if-range)# port-group 3 SwitchB(config-if-range)# exit SwitchB(config)# aggregateport load-balance dst-mac
Verification	● Run **show aggregateport load-balance** to check the load balancing algorithm configuration.
Switch A	SwitchA# show aggregatePort load-balance Load-balance : **Source MAC**
Switch B	SwitchB# show aggregatePort load-balance Load-balance : **Destination MAC**

.

7.5.4 Configuring Aggregated Port Configuration Delivery from the AC

Configuration Effect

- After the AC delivers the aggregated port configuration to the AP, the corresponding wired port on the AP will be added to or exit from the corresponding aggregated port.

Notes

- To ensure normal link aggregation, static AP member ports need to be configured consistently on the two devices over a link.
- After an AP member port is added to an aggregated port, the member port cannot be added to other aggregated ports. The member port can be added to another aggregated port only after it exits from the original AP port.

Configuration Steps

Configuring Aggregated Port Configuration Delivery from the AC

- Optional
- Perform this operation when a wired port of a specific AP, AP group, or all APs needs to be added to the AP aggregation group.

Command	**ap-interface wireport** *port-number* **port-group** *ap-number*
Parameter Description	**port-number**: Indicates the ID of the wired port on the AP. **ap-number**: Indicates the ID of the AP port.
Defaults	By default, the AC does not deliver aggregation port configuration.
Command Mode	ap-configure and ap-group configuration mode
Usage Guide	In ap-config and ap-group configuration mode, run **ap-interface wireport** *port-number* **port-group** *ap-number* to deliver an aggregated port configuration to enable a wired port on the AP to be added to the AP aggregation group, and run **no ap-interface wireport** *port-number* **port-group** for a specific wired port to exit from the AP aggregation group.

Verification

- Run **show running** to query the corresponding configuration.
- Run **show aggregateport summery** to query the corresponding relationship between the aggregated port and AP member ports.

Command	**show aggregateport summery**
Parameter Description	**ap-num**: Indicates the AP number.
Command Mode	All modes
Usage Guide	-
Command Presentation	FS# show aggregateport summary AggregatePort MaxPorts Ports ---------- -------- ---------- Ag1 8 Gi0/1,Gi0/2

7.6 Monitoring

Displaying

Description	Command

Description	Command
Displays the summary or load balancing algorithm of an AP port.	**show aggregateport** [*ap-number*] { **load-balance** | **summary** }

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs an AP port.	**debug lsm ap**

8 Configuring VLAN-TERMINAL

8.1 Overview

VLAN-TERMINAL accomplishes the one-armed router function. It is generally used in the hotel scenario, in which one VLAN is configured for each guest. When no sub port is configured, the traffic of each VLAN can be transmitted and received via a designated LAN port. Alternatively, traffic of the VLAN with a designed VID or in a designated VID segment can be transmitted and received via the same LAN port.

VLAN-TERMINAL facilitates network management and saves IP address resources. With fewer routers, network maintenance becomes convenient. Because VLAN IP addresses are in same network segment, workload caused by an increase or change of IP addresses decreases.

8.2 Applications

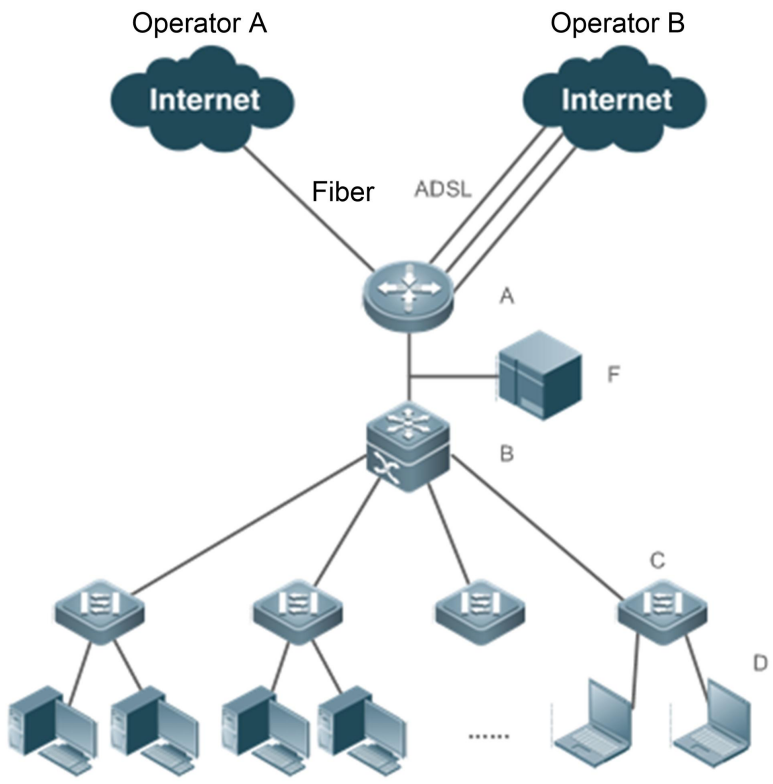
Application	Description
Deploying Egress Gateway	Deploys the VLAN-TERMINAL function on the egress gateway.

8.2.1 Deploying Egress Gateway

Scenario

In the hotel scenario, only one LAN port (physical port) on the egress gateway is connected to the switch. One VLAN is configured for each room. The switch does not provide the super VLAN function, and the mirroring port of the switch is connected to the network monitoring product that monitors each VLAN.

Figure 7–1 Typical Egress Gateway Application in Hotel Scenario



Remarks	A: egress gateway B: core switch C: switch D: client in the hotel room F: network monitoring product

Deployment

1. Basic NAT: Implement basic network address translation (NAT) to ensure that clients access the Internet normally.
2. Multi-link load balancing: Distribute traffic of data flows to multiple links to ensure proper utilization of bandwidth.
3. Configure VLAN-TERMINAL so that packets carrying different tags are forwarded via the same port.

8.3 Features

Basic Concepts

↘ VID

VID refers to the VLAN ID and is used to differentiate VLANs.

Overview

Feature	Description
VLAN-TERMINAL	Enables packets carrying different tags to be forwarded via the same port.

8.3.1 VLAN-TERMINAL

VLAN-TERMINAL facilitates network management and saves IP address resources. With fewer routers, network maintenance becomes convenient. Because VLAN IP addresses are in same network segment, workload caused by an increase or change of IP addresses decreases.

Working Principle

VLAN-TERMINAL is transparent to other functional modules, and does not affect data streams of other modules. With CLI configuration, the device driver can receive tagged packets with corresponding VIDs from the switch. These packets are resolved, have their tags removed, and are saved. Because these packets no longer contain tags, subsequent modules consider these packets as common packets and process them. When these packets need to be sent, the modules find corresponding tags based on the stream information and the mapping relationship, and tag the packets.

Related Configuration

Enabling VLAN-TERMINAL

VLAN-TERMINAL is disabled by default.

Run the **vlan-terminal enable** command in global configuration mode to enable VLAN-TERMINAL.

Run the no **vlan-terminal enable** command in global configuration mode to disable VLAN-TERMINAL.

Configuring Maximum Number of Concurrent Online Clients Belonging to Same VLAN

The maximum number of concurrent online clients corresponding to the same VID is 100 by default.

Run the **vlan-terminal per-vlan** *num* command to adjust the maximum number of concurrent online clients in the range 1–1000.

Run the no **vlan-terminal per-vlan** command in global configuration mode to delete related configuration.

Configuring VIDs on Corresponding Ports

Configure VIDs on corresponding ports (LAN ports only).

Run the **vlan-terminal vlan-list** *vlan-list* command in interface configuration mode.

Run the no **vlan-terminal vlan-list** command to delete related configuration.

8.4 Limitations

EG2000CE supports VLAN-TERMINAL module; EG3000XE and EG3000UE do not support VLAN-TERMINAL module.

8.5 Configuration

Configuration	Description and Command	
Enabling VLAN-TERMINAL	Mandatory	
	vlan-terminal enable	Enables VLAN-TERMINAL.
Configuring Maximum Number of Concurrent Online Clients Belonging to Same VLAN	Optional	
	vlan-terminal per-vlan *num*	Configures the maximum number of concurrent online clients corresponding to the same VID, with the value in the range 1–1000.
Configuring VIDs on Corresponding Ports	Mandatory	
	vlan-terminal vlan-list *vlan-list*	Configures VIDs on corresponding ports (LAN ports only). There may be only one VID or consecutive VIDs separated by the comma.

8.5.1 Enabling VLAN-TERMINAL

Configuration Effect

- Enable VLAN-TERMINAL to forward packets carrying different tags via the same port.

Notes

- This function is invalid if the VLAN-TERMINAL switch is disabled.

Configuration Steps

- Run the **vlan-terminal enable** command in global certification mode.

Verification

- Check the configuration status of VLAN-TERMINAL.

Related Commands

Enabling VLAN-TERMINAL

Command	**vlan-terminal enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Enabling VLAN-TERMINAL

Configuration Steps	Enable VLAN-TERMINAL on the egress gateway (device A).
	FS# configure terminal FS(config)#vlan-terminal enable
Verification	● Check the configuration status of VLAN-TERMINAL.
	FS#show vlan-terminal vlan-terminal: enable

8.5.2 Configuring Maximum Number of Concurrent Online Clients Belonging to Same VLAN

Configuration Effect

- Configure the maximum number of concurrent online clients corresponding to the same VID. If the number of concurrent online clients corresponding to the same VID reaches the maximum value, no other clients corresponding to the same VID can go online.

Notes

- This function is optional.
- The maximum number of concurrent online clients corresponding to the same VID is 100 by default. This value can be adjusted in the range 1–1000

Configuration Steps

- Run the vlan-terminal per-vlan num command in global configuration mode to configure the maximum number of concurrent online clients belonging to the same VLAN.

Verification

- Check the maximum number of concurrent online clients belonging to the same VLAN.

Related Commands

Configuring Maximum Number of Concurrent Online Clients Belonging to Same VLAN

Command	**vlan-terminal per-vlan** *num*
Parameter Description	num: Indicates the maximum number of concurrent online clients belonging to same VLAN. Once the number of concurrent online clients corresponding to the same VID reaches this value, no other client corresponding to the same VID can go online. The value ranges from 1 to 1000.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Setting Maximum Number of Concurrent Online Clients Belonging to Same VLAN to 30

Configuration Steps	Set the maximum number of concurrent online clients belonging to same VLAN to **30** on the egress gateway (device A).
	FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# vlan-terminal per-vlan 30
Verification	● Check the configuration information.
	FS#show vlan-terminal vlan-terminal: enable per-vlan: 30

8.5.3 Configuring VIDs on Corresponding Ports

Configuration Effect

- Designate a port via which packets corresponding to a VID are forwarded.

Notes

- If the configured VID conflicts with a sub port, the sub port prevails.

Configuration Steps

- Run the vlan-terminal vlan-list vlan-list command in interface configuration mode to configure VIDs on corresponding ports.

Verification

- Check the configuration information.

Related Commands

Configuring VIDs on Corresponding Ports

Command	**vlan-terminal vlan-list** *vlan-list*
Parameter Description	*vlan-list*: Indicates a single VID or consecutive VIDs separated by the comma.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuring VIDs 2, 5, 40–80, and 100–120 on Port 0/1

Configuration Steps	Configure VIDs 2, 5, 40–80, and 100–120 on Port 0/1 on the egress gateway (device A).
	FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# interface gigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# vlan-terminal vlan-list 2，5，40-80，100-200
Verification	● Check the configuration information.
	FS#show vlan-terminal vlan-terminal: enable per-vlan: 30 Gi0/1: 2,5,40-80,100-200

Common Errors

- The port attribute is incorrect (only LAN ports are supported).
- The format is incorrect.
- VIDs conflict.

8.6 Monitoring

Displaying

Description	Command
Displays the number of concurrent online clients corresponding to the same VID, and the IP addresses of the online clients corresponding to the VID.	**show vid-info**
Displays the VLAN-TERMINAL configuration information.	**show vlan-terminal**

https://www.fs.com

The information in this document is subject to change without notice. FS has made all efforts to ensure the accuracy of the information, but all information in this document does not constitute any kind of warranty.

Copyright © 2009-2022 FS.COM All Rights Reserved.